The Care Provider ALLIANCE

NHS Digital

INFORMATION GOVERNANCE TOOLKIT VERSION 14.1:

A HOW-TO-GUIDE FOR CARE PROVIDERS

Version 1 – July 17

Information Governance Toolkit v14.1: A How-To Guide for Care Providers

Introduction

This guide is not only aimed at smaller Care Homes, both residential and nursing, but also may be of use for other Social Care Providers e.g. Domiciliary Care.

The intention is that the nominated Information Governance (IG) Lead from each Care Provider can use this How-To Guide to achieve compliance with the IG Toolkit for their organisation.

The IG Toolkit is made up of requirements which are split into different Levels. Each requirement focusses on a specific aspect of Information Governance. The Levels are described in the table below. The Levels build on each other, for example, in order to reach Level 2, you must have also met the Level 1 requirements.

ATTAINMENT LEVELS	
0	There is insufficient evidence to attain Level 1.
1	The organisation has begun to plan the policies, procedures, processes and/or controls that are necessary to become compliant.
2	There are approved and implemented IG policies, procedures, processes or controls in place that have been made available to all relevant staff.
3	Staff compliance and the effectiveness of the policies, procedures, processes or controls is monitored and assured.

For the IG Toolkit, the required 'satisfactory' standard is defined as Level 2 across all applicable criteria.[1]

However, Care Providers are encouraged to carry out a "baseline" assessment the first time they complete the Toolkit. This will help identify any requirements on which more work is required, and therefore might include some Level 1s and 0s.

How to use this guide

This guide is aimed at helping you to work logically through the IG Toolkit.

It is best practice, and key evidence for Care Quality Commission (CQC) inspection, that all Health and Social Care organisations have a Quality Assurance system in place – *e.g.* policies and procedures.

CQC KLOE Well-Led 4.2 asks
"Are quality assurance and clinical governance systems effective, and are they used to drive continuous improvement?"

This guidance presumes that your organisation will have a policy and procedure system in place, whether this is something which has been developed in-house or provided to you by a supplier.

For many of the requirements, we have provided template policies and procedures or other templates which may help you with evidencing your attainment of each Level. These templates are not intended to be prescriptive – if you have policies or procedures in place which say the same thing then continue to use your existing systems.

In all cases, you should amend the templates or your existing policies and procedures to match your specific circumstances.

[1] Some of the requirements will not be applicable, e.g. those relating to NHS smartcards.

IG Toolkit – Key Facts

1. There are different "views" of the Toolkit dependent on organisation type. *i.e.* hospitals have to complete more requirements than a pharmacy. There is **not** a specific Care Provider version of the toolkit but most Care Providers are regarded as Voluntary Sector Organisations (VSOs) for the purposes of the IG Toolkit. **This is true whether your organisation is privately owned or indeed a voluntary body.**

2. Larger groups potentially could be set up as Any Qualified Provider (AQP) or NHS Business Partner when registering with the Toolkit [see below]. This is due to the type of contract from your commissioner or reflective of your organisation's size. AQP assessments have more requirements than VSOs in order to fulfil their contractual requirements. If you are an AQP or NHS Business Partner and need additional help, there is a resources and support list in the *Introduction to Information Governance for Registered Managers*.

3. The Toolkit has Levels 0-3, and the current standard for compliance is Level 2 in all applicable requirements. To complete a Level, you must satisfy all criteria associated with it, these are labelled "a", "b", "c" etc.

4. The first time you work through the Toolkit, you can complete a "baseline assessment" which might contain some Level 0s and 1s. This will help you generate an improvement plan for the future. This is also the minimum requirement for beginning the process of getting NHSmail.

5. Level 3 is not a requirement for Care Providers, but is considered good practice and some may have already reached this level in some areas.

6. There may be some requirements that are not relevant to your organisation *e.g.* requirement 304 is only relevant if your organisation uses NHS Smartcards. If a requirement is not relevant you can check the "Not Relevant" box on the IG Toolkit. Not all requirements have a "Not Relevant" option, however, if you determine that you need an exemption for your organisation this can be requested via the IG Toolkit Help Desk and a form will be provided.

7. Each requirement asks that your organisation can evidence that you fulfil the criteria. It is not mandatory that you upload this evidence to the IG Toolkit as long as you can state where the information can be found in your organisation. However, it is considered best practice to upload evidence or to provide a thorough commentary and signposting of evidence.
8. **It is essential that you work through the Levels of the IG Toolkit systematically, modifying or creating your policies and collecting evidence as you go, rather than seeking to immediately bring everything into place without consideration and necessary amendment.**

Maintaining Information Governance Compliance

Once you have completed the IG Toolkit, you will need to periodically review your IG compliance – at least once a year.

This guidance is based on version 14.1 of the Toolkit but there are usually some changes to the criteria each year. The following questions have been designed to help you develop a robust plan for compliance going forward:

1. How has your CQC inspection gone?
2. Has National Policy changed *e.g.* Have the 10 Data Security Standards become regulatory?
3. Have there been any changes to legislation or supporting guidance? e.g. Wider legislation will be changing in 2018 as the General Data Protection Regulation (GDPR) passes into law, superseding the Data Protection Act 1998. See https://ico.org.uk/ for advice.
4. Revisit the decisions you took about how you implemented IG in your organisation – have you got the right resources deployed?
5. Have you incorporated any improvements from spot checks into your improvement plan?
6. The IG Toolkit will be re-designed in 2018 to incorporate more cyber security elements. How will this change the policies you currently have in place?

Starting the IG Toolkit

The IG Toolkit Version 14.1, VSO View – Step-by-Step

The following pages set out the requirements of the IG Toolkit in order. Regular text is taken from the IG Toolkit v.14.1 itself. The bold, italicised text in blue is our more in-depth and tailored guidance on what is required.

At the end of each requirement there is a list of resources which may help you with fulfilling each criterion. These are template policies, procedures and forms, exemplar text to insert into contracts or service user handbooks, or hyperlinks to webpages which have detailed advice on how to complete the specific task. Space has also been made for your comments, if required.

In the event that you need additional support beyond what is available in this guidance, the IG Toolkit website has an extensive knowledge base of materials which may be of use to you. Equally, each requirement has extensive guidance on the IG Toolkit website. Some of this guidance will not apply to Care Providers as it has a broader focus on the entire Health & Social Care sector.

Throughout, we have pointed to CQC Key Lines of Enquiry (KLOEs) which align with Toolkit requirements. These are the new KLOEs which will come into effect from October 2017. This has been intended to help prevent duplication of effort in your organisation. This does not mean that all relevant KLOEs have been pointed out; for example,

KLOE Effective 4.5 "How is technology and equipment used to enhance the delivery of effective care and treatment and to support people's independence?"

may well be relevant for some organisations who have implemented a lot of technology in their service but won't be relevant for others. Also, it does not relate directly to any of the IG Toolkit criteria, so therefore has not been included in this *Guide.*

How to Log in and Use the IG Toolkit:

Your first step will be to go to the IG Toolkit website: https://www.igt.hscic.gov.uk/.

You need to register for a user account on behalf of your organisation. If you are an organisation with multiple sites, it would be a head office decision whether you complete the IG Toolkit at each location or if this would be completed by the parent organisation on behalf of all sites. Please note though that where the latter option is chosen the submission must state which sites are covered, in the section: *"View organisations which this assessment covers."*

There are instructions on how to register on the website homepage: https://www.igt.hscic.gov.uk/resources/UserGuide-HowToRegister.pdf.

You will need to know your Organisation/ODS Code to register, and in order to have one you must be on the Health and Social Care Organisations database. Your code can normally be found here: https://digital.nhs.uk/organisation-data-service/data-downloads. If for any reason you are not on this database, you will need to ask to be registered by following the instructions on the registration page.

You will receive your User ID and password by email – normally within 48 hours. Use your ODS code, User ID and password to log in to the IG Toolkit.

There is a "Quick Start Guide" on how to use the IG Toolkit on their homepage:https://www.igt.hscic.gov.uk/resources/IG%20Toolkit%20Quick%20Start.pdf. This guidance has hints and tips on how the IG Toolkit works and how it can be navigated.

How to Publish your IG Toolkit Submission:

Once you have completed all the requirements and your assessment has been signed off by Senior Management you should then be able to 'Publish' your assessment.

There is detailed guidance on how to do this here: https://www.igt.hscic.gov.uk/resources/UserGuide-HowToCompleteAssessment_GPs-Pharmacies.pdf.

Once you have completed all requirements, a yellow ‘Publish’ button will appear on the Assessment Summary Page. By Clicking ‘Publish’ you are confirming that your Senior Management team has signed off this assessment and no other changes are required. Clicking the publish button means that your assessment will **immediately** be published on the IG Toolkit website via the IGT Reports section and your scores (not the comments or evidence) will therefore be accessible to others.

Once you have done this, read the ‘IG Assurance Statement’, and scroll down the page to ‘Accept’ the Statement. Once you have accepted, your assessment will be fully published and the system will send you an email to confirm your assessment publication has been received.

114	**Responsibility for Information Governance has been assigned to an appropriate member, or members, of staff.**	
<u>Level 1.</u> Responsibility for Information Governance has been assigned and an IG improvement plan has been developed.	a	Responsibility has been assigned for Information Governance. ***Someone within your organisation should become the Information Governance (IG) Lead. Note that the IG Lead does not have to be the Registered Manager. The Lead has 2 key areas of responsibility:*** ***1. Responsibility for managing information risks.*** ***2. Responsibility for ensuring the respect of the rights of service users*** ***Senior management need to consider whether the responsibilities can be met by one member of staff or whether this should be shared.*** ***In larger organisations, the role of the IG Lead is often split between a SIRO and a Caldicott Guardian, in SMEs it is not necessary to have 2 distinct roles.*** <u>Evidence (recommended but not mandatory):</u> Named individual(s) job description(s), or a signed note or e-mail assigning responsibility.
	b	The named Information Governance leads have been provided with sufficient training to carry out their role. ***The IG Lead(s) needs to be sufficiently trained to undertake their responsibilities. Training should cover the Data Protection Act 1998, the Caldicott principles, security, confidentiality, and appropriate information sharing - training can be in-house training packages/commercial training companies or training provided by the commissioning organisation. Each site should consider how the IG Lead will be trained and if it is appropriate***

		for them to also become a registered Caldicott Guardian [more information below]. *The IG Training Tool (IGTT) was decommissioned on 31st December 2016 pending the development of new training; however, there is a workbook on the IG Toolkit website, though it is not aimed at Care Providers, and there is more information about IG available in the resources list in the Introduction to Information Governance for Registered Managers.* *As a first training step, IG Lead(s) should have read and understood the Introduction to Information Governance for Registered Managers.* <u>Evidence (recommended but not mandatory):</u> IG Training Tool reports, certificates of attendance and attainment, or evidence of self-directed study.
	c	There is an IG improvement plan that documents both the current level of compliance with the NHS IG requirements and the targets identified to progress to the next level of compliance. *To create a plan, you need to work through each IG Toolkit requirement and consider your current compliance status and your next steps to improve. By setting targets and entering comments on the IG Toolkit an improvement plan is automatically generated. The IG Toolkit improvement plan will help you assess your current compliance and decide your next steps. Completing this for the first time is your "Baseline Assessment" which is the minimum requirement for obtaining NHSmail.*

		Evidence (recommended but not mandatory): Documented IG improvement plan.
Level 2. The IG improvement plan has been approved by a senior staff member and is being implemented.	a	The IG improvement plan has been signed-off by a senior staff member. ***This may be board-level sign off, or sign off from your IG Lead. The important part here is to ensure that the plan has been seen and approved so that steps can be made to improve IG in your organisation, not the organisational structure.*** ***Throughout the Toolkit, reference is made to sign-off by a senior staff member and you will know who this most accurately describes in your organisation.*** Evidence (recommended but not mandatory): Sign off should be documented on the IG improvement plan, for example the date that it was signed-off and by whom.
	b	The IG improvement plan has been implemented and gaps or weaknesses in current IG arrangements are being addressed. Evidence (recommended but not mandatory): New guidance for staff or new organisational procedures or new ways of working. ***e.g. Evidence of changes to induction pack/confidentiality policies &c.*** ***If you chose to utilise the template policies and procedures in the resources provided, evidence that these have been altered to suit the needs of your organisation is sufficient.***

Level 3. In-year reports and briefings on progress against the improvement plan are provided to senior management. IG arrangements are reviewed by a senior member of the organisation on at least an annual basis.	a	Progress against the improvement plan is monitored in-year and reports are made to senior members of staff. ***It is important to note that Level 3 is always about ongoing annual audits and monitoring of policies. It is important that your organisation reviews its IG policies and procedures annually to make sure that you continue to comply with all new legislation and requirements.*** ***P. 4 of this guide has hints on how to ensure ongoing IG compliance.*** Evidence (recommended but not mandatory): Progress reports or briefing documents or meeting notes or emails. ***This can be a copy of your updated improvement plan. This must be dated.***
	b	[Only required if Attainment Level 3 was achieved in the previous assessment] The adequacy of the IG arrangements needs to be reviewed at least annually to ensure they remain fit for purpose. ***We have provided an annual Information Governance Audit Checklist – [03] -as a reminder to review.*** Evidence (recommended but not mandatory): Minutes/meeting notes including the decisions made and any changes required. ***Dates of annual review must be recorded.***

Resources:	- ***More information about Caldicott Guardians is available here:*** https://www.gov.uk/government/groups/uk-caldicott-guardian-council - ***More information about SIROs is available here:*** https://digital.nhs.uk/organisation-data-service/our-services - [03] ***Annual IG Audit Checklist (Internal)***
Comments:	

115	**There is an Information Governance policy that addresses the overall requirements of Information Governance**	
Level 1. Current policies have been reviewed to determine where they can be adapted to form the basis of an Information Governance policy, which should underpin the organisation's IG improvement plan (see requirement 114).	a	The IG lead(s) has/have reviewed current policies to determine where they can be adapted to form the basis of an Information Governance policy. ***In the instance that your organisation does not already have an overarching Information Governance policy, a template which can be easily adapted has been provided – [01].*** ***CQC KLOE Well-Led 2 "Does the governance framework ensure that responsibilities are clear and that quality performance, risks and regulatory requirements are understood and managed?"*** ***And*** ***Well-Led 2.8 "How does the service assure itself that it has robust arrangements to ensure the security, availability, sharing and integrity of confidential data, and records and data management systems?"*** Evidence (recommended but not mandatory): An IG policy document tailored to the requirements of the organisation.
	b	The IG policy has been signed off by a senior member of the organisation. Evidence (recommended but not mandatory): Sign off documented on the policy document (e.g. the date that it was signed-off and by whom).

Level 2. The approved IG policy has been made available to all members of the organisation's staff.	a	The IG policy has been made available to all members of organisation's staff. ***We have provided example texts which you may like to insert into your staff handbook or to utilise as part of your staff induction process – [02]. All policies which are relevant to staff working should be made available to them.*** Evidence (recommended but not mandatory): Inclusion in a staff handbook or by placing it on the Intranet, or staff may be provided with their own copy of the policy. In the latter case, there may be a list of staff signatures confirming staff have read and understood the policy.
Level 3. Staff compliance with the IG policy is monitored and assured.	a	Staff understanding of the policy and its relevance to the way they work is tested to ensure that there is full compliance with the IG policy. Therefore, compliance spot checks and routine monitoring are conducted. ***We have provided an annual audit check list for the IG Lead which can be used to evidence ongoing monitoring of IG within an organisation. This should be done on a rolling basis and is not designed to be completed in one day – [03]. Our Introduction to Information Governance for Staff also has a short test which can be used as part of your compliance monitoring.*** Evidence (recommended but not mandatory): Completed monitoring form, or a report on the outcome of staff compliance checks.

	b	[Only required if Attainment Level 3 was achieved in the previous assessment] The adequacy of the IG policy needs to be reviewed regularly to ensure it remains fit for purpose. Evidence (recommended but not mandatory): Minutes/meeting notes including the decisions made and any changes required.
Resources:	- [01] ***Information Governance Policy - Template*** - [02.1] ***Staff Handbook – Exemplar Text*** - [03] ***Annual IG Audit Checklist (Internal)***	
Comments:		

116	**All contracts (staff, contractor and third party) contain clauses that clearly identify Information Governance responsibilities.**	
Level 1. Action has been taken to determine whether contracts of staff, contractors and third parties contain clauses setting out IG responsibilities.	a	An audit of personnel records, and contractor and other third party contracts has been undertaken to determine how many have written contracts that contain clauses that identify IG responsibilities. Evidence (recommended but not mandatory): A list of staff (including temps, locums, students and volunteers), contractors and third parties with access to personal information.
	b	Appropriate contractual clauses covering compliance with IG linked to disciplinary procedures (where appropriate) have been drafted and signed off by senior management. ***We have provided example clauses for insertion into current staff contracts if required. You will need to consider how you will ensure that agency staff understand and comply with IG procedures.*** ***There is more information on the Government's website on how to legally update contracts. The link is in the resource box below.*** Evidence (recommended but not mandatory): Examples of contract clauses. Meeting notes showing approval or personal endorsement in writing (e.g. by email) from an appropriate senior manager.

	c	An action plan has been developed to update existing contracts, where necessary, and ensure all new contracts include compliance with IG requirements as part of employment/service engagement processes. Evidence (recommended but not mandatory): Documented action plan.
Level 2. Appropriate clauses on compliance with IG have been put into all contracts and/or agreements.	a	Building upon the existing contractual situation, all contracts for staff, contractors and other third party users who have access to confidential information or assets containing confidential information include compliance with Information Governance requirements, as part of employment or contracting processes. ***We have provided a template Non-Disclosure Agreement for Third Party/Contractor use.*** ***Consider who in your organisation has access to confidential information, will you need to update the contracts of everyone who works in your organisation? Or just some? Some third party suppliers will already be used to having confidentiality or information governance clauses in their contracts and so may already be covered.*** Evidence (recommended but not mandatory): Sample contract showing that appropriate IG clauses are included in contracts. ***Note that you should evidence both staff and third party contracts.***

Level 3. Compliance with the clauses is monitored and assured. Formal contractual arrangements with staff, contractors and third parties are reviewed regularly.	a	All new staff, contractor and other third parties comply with IG responsibilities and this is tested through spot checks and routine monitoring. ***We have provided an annual audit check list for the IG Lead which can be used to evidence ongoing monitoring of IG within an organisation. This should be done on a rolling basis and is not designed to be completed in one day – [03].*** Evidence (recommended but not mandatory): Completed monitoring forms, or a report on the outcome of staff compliance checks.
	b	[Only required if Attainment Level 3 was achieved in the previous assessment] As the law in this area is subject to change, an annual review is undertaken to assess whether the contractual clauses are still sufficient. Evidence (recommended but not mandatory): Meeting notes including the decisions made and any changes required.
Resources:		• [03] ***Annual IG Audit Checklist (Internal)*** • [04] ***Staff Contracts – Exemplar Text*** • [05] ***Third Party Contract – Non-Disclosure Agreement – Template*** • ***Information on how employment contracts can be changed can be found here:*** https://www.gov.uk/your-employment-contract-how-it-can-be-changed

Comments:	

117	**All staff members are provided with appropriate training on Information Governance requirements**	
<u>Level 1.</u> Appropriate IG training has been identified that includes induction for new starters.	a	Responsibility for arranging appropriate IG training for all staff has been assigned to a named individual. ***There may be some overlap in the evidence for this requirement with 114, 115 and 216.*** <u>Evidence (recommended but not mandatory)</u>: A named individual's job description, or a signed note or e-mail assigning responsibility.
	b	Appropriate basic IG training has been identified for all staff including new starters, and additional training has been identified for key staff groups. ***Training must be provided to all existing staff as well as any new starters. Included in this guidance pack is an Introduction to Information Governance for Staff which may be included in your training plans. This summary also has 4 case studies which can be used to quiz staff to ensure they have understood the contents.*** ***N.B. a lot of the IG training available refers to the Freedom of Information Act 2000 which may not be applicable for your organisation.*** ***We have also included updates which should be made to staff handbooks – [02].***

		CQC KLOE Caring 3.3. "How does the service make sure that staff understand how to respect people's privacy, dignity and human rights?" Evidence (recommended but not mandatory): Written details of the training to be provided.
	c	Basic IG training is provided to all new starters as part of their induction. ***The IG Training Tool (IGTT) was decommissioned on 31st December 2016 pending the development of new training; however, there is a workbook on the IG Toolkit website, though it is not aimed at Care Providers, and there is more information about IG available in the resources list in the Introduction to Information Governance for Registered Managers.*** Evidence (recommended but not mandatory): Training records, for example, IG Training Tool reports, training certificates of attendance or attainment.
Level 2. All staff members have completed or are in the process of completing IG training. Training needs are	a	All staff including locum, temporary, volunteer, student and contract staff members have completed or are in the process of completing basic IG training. ***You should consider how you will ensure that agency staff understand and follow IG procedures. It may be best to ensure your contract with the agency stipulates that they receive training from the agency.*** Evidence (recommended but not mandatory): Training reports or certificates of attendance.
	b	The training needs of staff is assessed to ensure that the basic training provided is sufficient and staff in key roles are provided with additional training

regularly reviewed and re-evaluated when necessary.		when required which may be provided through the NHS IG Training Tool or by other means. ***IG training should be part of your mandatory training matrix as IG breaches can be regulated both at company and at an individual staff level. As the Training Tool has been decommissioned other training will have to be identified.*** <u>Evidence (recommended but not mandatory)</u>: Training needs analysis document, certificates of attendance / attainment or IG Training Tool reports.
<u>Level 3.</u> Action is taken to test and follow up staff understanding of IG and additional support is provided where needs are identified. Training provision is regularly	a	Providing staff with IG training does not provide sufficient assurance that they have understood their IG responsibilities. Therefore, compliance checks and routine monitoring is undertaken to test staff understanding and to ensure procedures are being complied with, where necessary, actions are taken. ***We have provided an annual audit check list for the IG Lead which can be used to evidence ongoing monitoring of IG within an organisation. This should be done on a rolling basis and is not designed to be completed in one day – [03].*** <u>Evidence (recommended but not mandatory)</u>: A completed audit sheet or monitoring form, or a report on the outcome of staff compliance checks and any actions taken.
	b	Where necessary, any staff member requiring assistance should be supported to increase their understanding of and adherence to IG best practice.

reviewed.		<u>Evidence (recommended but not mandatory)</u>: Training attendance lists, diary slots for individual training, HR/personnel records, or staff signature lists - that staff have received additional support and understand their duties and responsibilities.
	c	[Only required if Attainment Level 3 was achieved in the previous assessment] Staff understanding and training materials are regularly reviewed especially when new procedures are introduced and on induction of new staff. <u>Evidence (recommended but not mandatory)</u>: Meeting notes where the training was reviewed during the year including the decisions made and any updates.
Resources:	• [02] ***Staff Handbook – Exemplar Texts*** • [03] ***Annual IG Audit Checklist (Internal)*** • ***Introduction to Information Governance for Staff*** • ***There is a workbook on the IG Toolkit website which may be helpful for staff training – note that this has not been aimed at Care Providers specifically.***	
Comments:		

202	**Confidential personal information is only shared and used in a lawful manner and objections to the disclosure or use of this information are appropriately respected**	
<u>Level 1.</u> The organisation must have a plan of action for identifying all purposes that involve the sharing or use of confidential personal information and for determining the legal basis for such sharing or use.	a	There is a documented plan for identifying all purposes supported by confidential personal information and for determining the legal basis for each. ***The purpose of this is for you to identify all confidential personal information that is used or shared by your organisation so that you can ensure you are complying with the law when using and sharing the information. This means identifying types of information rather than individual service user records. For example, service user records might be shared with a local NHS hospital for direct care purposes and with the person's consent.*** <u>Evidence (recommended but not mandatory)</u>: The documented plan.
	b	The plan has been approved by senior management, an appropriate committee or other established local governance process. <u>Evidence (recommended but not mandatory)</u>: Minutes of meetings, in a document or email or a personal endorsement in writing from an appropriate senior manager.
<u>Level 2.</u> All purposes	a	There are guidelines for staff that are accessible to them in an appropriate location.

that require confidential personal data to be used or shared have been identified and have a clear and documented lawful basis. All staff engaged in supporting these purposes understand what is lawful and what is not.		***We have provided exemplar text [02] to insert into your staff handbook. Note that your staff handbook must state where staff can access policies and procedures regarding IG and that staff have signed to acknowledge receipt of this information.*** Evidence (recommended but not mandatory): Inclusion in staff handbook, or published on the Intranet, or personal copies for staff (in the latter case there may be a list of staff signatures confirming receipt of the guidance) or the evidence may be a description of the dissemination process or minutes of the meeting where this was decided.
	b	All flows and uses of confidential personal information have been identified and documented and the underpinning legal basis is clearly understood and recorded. For advice on how information mapping works, there is a link to extensive advice and examples in the resource box below. ***This information can be kept within an Information Asset Register (IAR), a template has been provided – [07].*** ***Note that the IAR is not just about recording pieces of computer equipment, but also a place to note what software is being run i.e. Windows 10 etc. You should also keep a record in the IAR about paper documents. It should record all types of information and how it is stored.*** ***Importantly, for all confidential personal information the IAR must record:***

		• ***What the information is used for,*** • ***If relevant, who it is shared with, and*** • ***The legal basis for using or sharing the information.*** Evidence (recommended but not mandatory): Document or spreadsheet that captures the required information. This may be achieved by adding to the organisation's information asset register. Notes or minutes of team meetings/awareness sessions or staff briefing materials.
	c	All uses and sharing of confidential personal information that do not have a clear legal basis are treated as data breaches and have been reported to the Board and to NHS Digital via the IG SIRI Incident Reporting Tool. ***Your organisation may not have a Board but it is important that there is a documented strategy in place stating who should be informed in the case of a data breach.*** ***We have provided a link to NHS Digital's advice on correct incident reporting procedures. We have also created an Information Security Incident Report Form – [11] – for internal use.*** ***Your organisation should have a disciplinary procedure in place around data breaches, and a procedure for reporting severe breaches to the IG Incident Reporting Tool. This will automatically report severe breaches to the Information Commissioner's Office (ICO).***

		Evidence (recommended but not mandatory): Copies of all such breaches reported OR Add a comment stating that there have been no such breaches. Meeting notes where such a breach was discussed OR Meeting notes from an appropriate governance body that clearly state that there have been no such breaches.
Level 3. The organisation ensures that it respects service user objections in respect of the use and sharing of confidential personal information unless there is a legal basis that overrides an individual's objection.	a	The organisation must ensure that it has a process in place for managing and responding to any objections made by service users in respect of the use or sharing of confidential personal information. ***We have provided exemplar text to insert into your General Consent on Admission form for service users – [08]; however, you will have to insert your organisation's own procedures into this document.*** ***We have also provided a leaflet – [10] - which is aimed at informing service users about their rights in terms of confidentiality. You can update this leaflet to reflect your organisation's policies.*** Evidence (recommended but not mandatory): Documented process.
	b	It is important to ensure that information is shared in compliance with the law and is in line with the expectations of the public. Satisfaction surveys and focus groups are used to check that service users understand their consent choices and feel that their wishes are respected. Evidence (recommended but not mandatory): Completed satisfaction surveys that evidence that service users understand their rights and options.

		This may well be the same survey that you use for the "Caring" KLOEs. Notes of focus group meetings that evidence that service users understand their rights and options.
	c	[Only required if Attainment Level 3 was achieved in the previous assessment] Policy and law change over time and it is important that uses of data and guidance are regularly reviewed and aligned with the latest central guidelines. ***We have provided an annual audit check list for the IG Lead which can be used to evidence ongoing monitoring of Information Governance within an organisation. This should be done on a rolling basis and is not designed to be completed in one day – [03].*** Evidence (recommended but not mandatory): Minutes/meeting notes where the guidance has been reviewed during the year including the decisions made and any updates to the guidance. Notes of a review, completed during the assessment year, of data use and sharing and their underpinning legal bases.
Resources:	• ***A Staff Confidentiality Code of Conduct Template is available here:*** https://www.igt.hscic.gov.uk/KnowledgeBaseNew/HSCIC_AQP%20Template_Staff%20Confidentiality%20Code%20of%20Conduct.doc • [02] ***Staff Handbook – Exemplar Texts*** • [03] ***Annual IG Audit Checklist (Internal)*** • [06] ***Confidentiality Policy (including monitoring & auditing access) – Exemplar Texts*** • [07] ***Information Asset Register – Template***	

	• [08] ***General Consent on Admission Form – Exemplar Text*** • [10] ***Service User Leaflet*** • [11] ***Information Security Incident Report Form*** • ***Further information about Incident Reporting can be found here:*** https://www.igt.hscic.gov.uk/resources/The%20Incident%20Reporting%20Tool%20User%20Guide.pdf • ***Further information about Incident Reporting can also be found here:*** https://groups.ic.nhs.uk/TheInformationGovernanceKnowledgebase/The%20Information%20Governance%20Knowledgebase/Forms/Cyber%20Incident%20Reporting.aspx • ***Further information about information mapping can be found here:*** https://www.igt.hscic.gov.uk/DataMappingGuidance.aspx
Comments:	

<table>
<tr><th>209</th><th colspan="2">All person identifiable data processed outside of the UK complies with the Data Protection Act 1998 and Department of Health guidelines</th></tr>
<tr><td colspan="3">NR: This requirement may well not be relevant for your organisation as long as transfers of personal information have been reviewed and no overseas processing is carried out.
<b><i>The most likely reason for sharing information overseas is when a service user has next of kin outside of the UK. If this is the case, then it is important to carefully consider how you will share any information. If you have a Care Planning system which allows remote log on, perhaps the next of kin can log-in to the system from overseas without you having to send any information? If this is not an option, do you both have access to a secure email address? Do you send information via post?</i></b>
<b><i>Alternatively, if you have cloud based data storage, you need to find out from your supplier where in the world the servers which store any of your personal or sensitive information are kept.</i></b>
<b><i>There are complicated laws governing the transferral of data overseas and the IG Toolkit website gives an overview of the legislation. If you are uncertain the ICO also has guidance and a helpline.</i></b></td></tr>
<tr><td><u>Level 1.</u>
All transfers of personal information to countries outside the UK have been documented, reviewed and tested to</td><td>a</td><td>Responsibility has been assigned for reviewing information flows to identify overseas transfers.

<b><i>The responsible member of staff should be indicated in the appropriate location in your overarching Information Governance policy – [01]. We have provided links to guidance on creating Information Flows below. Should you require more assistance with this, the ICO should be contacted.</i></b>

<u>Evidence (recommended but not mandatory)</u>: A named individual's job description, or a note or e-mail assigning responsibility or the terms of</td></tr>
</table>

determine compliance with the Data Protection Act 1998 and Department of Health guidelines.		reference of a group.
	b	All identified transfers of personal data to a country outside the United Kingdom have been documented and reviewed for compliance with the Data Protection Act and Department of Health guidelines. ***The work for this requirement will overlap with the evidence provided in 202. You IAR should answer the following questions:*** ***1. What information is it?*** ***2. Who it is shared with?*** ***3. The legal basis for sharing the information.*** ***4. What is the method of transfer?*** ***In 2018 the General Data Protection Regulation (GDPR) will apply and will supersede the Data Protection Act 1998 (DPA). The UK's decision to leave the European Union will not affect the commencement of the GDPR. It is worth bearing in mind that the law will therefore be changing soon.*** ***We have provided an annual audit check list for the IG Lead which can be used to evidence ongoing monitoring of Information Governance within an organisation. This should be done on a rolling basis and is not designed to be completed in one day – [03].*** Evidence (recommended but not mandatory): A documented report detailing all personal information flows to overseas locations and the result of risk

		assessments undertaken. This must be updated annually.
<u>Level 2.</u> All transfers of personal data to countries outside of the UK fully comply with the Data Protection Act 1998 and DH guidelines. Where the review of overseas transfers reveals that appropriate contracts are not already in place for existing	a	All transfers of personal data to countries outside of the UK fully comply with the Data Protection Act 1998 and DH guidelines. Where the review of overseas transfers reveals that appropriate contracts are not already in place for existing transfers, new contractual terms that appropriately cover data protection and place restrictions on further use must be negotiated with recipient organisations. ***The ICO have drafted template contract clauses, the link is provided within resources.*** <u>Evidence (recommended but not mandatory)</u>: Minutes/meeting note or document detailing senior management sign off of overseas transfers with a clear statement that all requirements have been met.
	b	A review of current data processing and transfers has taken place during the current financial year and all changes to overseas transfers have been identified and new transfers assessed for compliance with the Data Protection Act 1998 and Department of Health guidelines. <u>Evidence (recommended but not mandatory)</u>: Refreshed evidence to satisfy attainment 1(b) and minutes/meeting note confirming the current position and continued compliance.

transfers, the organisation ensures that new contractual arrangements are signed.		
<u>Level 3.</u> Transfers of personal data to non-UK countries are regularly reviewed to ensure they continue to fully comply with the Data Protection Act 1998 and DH guidelines.	a	Transfers of personal data to non-UK countries are regularly reviewed to ensure continuing compliance. <u>Evidence (recommended but not mandatory)</u>: Documented details of the review of the transfers (e.g. checks that information is still being sent and received by the most secure method, and any decisions made to amend the transfer).
	b	[Only required if Attainment Level 3 was achieved in the previous assessment] Policy and law change over time as do technological advances and it is important that the overseas transfer of personal data continues to comply with the law and central guidelines. ***We have provided an annual audit check list for the IG Lead which can be used to evidence ongoing monitoring of IG within an organisation. This should be done on a rolling basis and is not designed to be completed in one day – [03].*** <u>Evidence (recommended but not mandatory)</u>: Minutes/meeting notes where

	the transfers, recipients and contracts have been reviewed during the year including the decisions made and any updates.
Resources:	• [01] ***Information Governance Policy – Template*** • [03] ***Annual IG Audit Checklist (Internal)*** • [07] ***Information Asset Register - Template*** • ***Guidance on what happens if you need to send personal data outside of the EEA is available here:*** https://ico.org.uk/for-organisations/guide-to-data-protection/principle-8-international/ ***This also includes information and links to model contract clauses. These can be found under the heading: "How can you use contracts to ensure there is an adequate level of protection?"*** • ***Guidance on when it is acceptable to share information is available here:*** https://ico.org.uk/for-organisations/guide-to-data-protection/data-sharing/ • ***Guidance on information mapping is available here:*** https://www.igt.hscic.gov.uk/datamappingguidance.aspx • ***Guidance on Cloud based computing is available here:*** https://www.ncsc.gov.uk/guidance/cloud-security-collection
Comments:	

213		**There is a publicly available and easy to understand information leaflet that informs patients/service users how their information is used, who may have access to that information, and their own rights to see and obtain copies of their records**
Level 1. Basic information about the use of personal data is made available to service users via a leaflet.	a	There is a documented leaflet that provides basic information on how personal information is used and shared in the organisation, and how service users can gain access to their own records. ***We have provided a leaflet which is aimed at service users [10], but which all staff should be aware of. This leaflet details how their personal information is used and shared and made available to them and has space for you to enter your organisation's policy and procedure around consent to share.*** ***CQC KLOE Caring 3.4 "How are people assured that information about them is treated confidentially and respected by staff?"*** Evidence (recommended but not mandatory): Documented leaflet.
	b	The leaflet has been approved by senior management. Evidence (recommended but not mandatory): Minutes of meetings, in a document or email or a personal endorsement in writing from an appropriately manager.
Level 2. Staff have been informed about	a	More comprehensive information is made available with appropriate service user communications and on request.

the communication material and there is more comprehensive information available to service users that require it.		*We have provided exemplar text which may be inserted into the service user handbook [09]. In the instance that a service user does not want to share their information, or that they are unhappy about how their information has been used, you should have a way for them to report this. This will both demonstrate that you are taking their concerns seriously, and also allow you to make improvements where necessary.* ***CQC KLOE Responsive 2.3 "Are concerns and complaints used as an opportunity to learn and drive continuous improvement?"*** Evidence (recommended but not mandatory): An example of the information sent to service users.
	b	To ensure that effective information is provided to service users, staff members are briefed about the content of the materials, and how to answer any detailed questions service users may have about use of their information or know who to refer the service user to. Evidence (recommended but not mandatory): Minutes/notes from team meetings, staff signature lists (that they have been informed) or briefing materials used in awareness sessions.
	c	Where necessary, communications materials are provided in different formats or by different routes to meet the need of service users with special or different needs. ***CQC KLOE Responsive 1.5 "Does the service identify and meet the information and communication needs of people with a disability or***

		sensory loss and does it record, highlight and share this information with others?" <u>Evidence (recommended but not mandatory)</u>: Tailored materials (where developed) for example large print, Braille, different languages. Details of the translation services that can be accessed e.g. email address, phone number.
<u>Level 3.</u> Service users are appropriately informed of how their information is used, who may have access to that information, and their own rights to see and obtain copies of their records. The communications	a	All written communications with service users include advice on the way that their information is used and shared, and how service users can gain access to their own records. Details of which staff member to approach for further assistance is also made available. <u>Evidence (recommended but not mandatory)</u>: An example of the written communications sent to service users.
	b	The purpose of informing service users about the use of personal information is to provide a basis for implying consent for using and sharing information for care purposes. Satisfaction surveys are used to check whether service users believe they are informed about uses of their personal information and that their questions are answered. <u>Evidence (recommended but not mandatory)</u>: Examples of completed surveys. ***This may well be the same survey that you use for the "Caring" KLOEs.***

materials are reviewed regularly to ensure they remain aligned with policy and legislation.	c	[Only required if Attainment Level 3 was achieved in the previous assessment] Policy and law change over time and it is important that the content of communications is regularly reviewed and aligned with the latest central guidelines. ***We have provided an annual audit check list for the IG Lead which can be used to evidence ongoing monitoring of IG within an organisation. This should be done on a rolling basis and is not designed to be completed in one day – [03].*** Evidence (recommended but not mandatory): Minutes/meeting notes where the materials have been reviewed during the year including the decisions made and any updates to the materials.
Resources:	• [03] ***Annual IG Audit Checklist (Internal)*** • [09] ***Service User Handbook – Exemplar Text*** • [10] ***Service User Leaflet***	
Comments:		

214	**There is a confidentiality code of conduct that provides staff with clear guidance on the disclosure of personal information**	
<u>Level 1.</u> There is a documented confidentiality code of conduct for staff that provides clear guidance on the disclosure of patient personal information and has been signed off by an appropriate senior manager.	a	There is a documented confidentiality code of conduct for staff that provides clear guidance on the disclosure of patient personal information. ***We have provided a link to a Staff Confidentiality Code of Conduct in the resource box below. If your organisation already has robust policies around confidentiality and disclosure of personal information, then these should continue to be in place.*** <u>Evidence (recommended but not mandatory)</u>: Documented confidentiality code of conduct.
	b	The code has been approved by senior management. <u>Evidence (recommended but not mandatory)</u>: Minutes of meetings, in a document or email or a personal endorsement in writing from an appropriate member of the senior staff.
<u>Level 2.</u> The code	a	The code is accessible to staff.

has been made available at appropriate points in the organisation and all staff members have been informed about the need to comply with it.		<u>Evidence (recommended but not mandatory)</u>: Inclusion in a staff handbook or by placing it on the Intranet, or staff may be provided with their own copy of the code. In the latter case there may be a list of staff signatures confirming receipt of the guidance.
	b	All staff members have been informed of the code and in particular of their own responsibilities for compliance. <u>Evidence (recommended but not mandatory)</u>: Minutes/notes of team meetings, or briefing materials used in awareness sessions.
<u>Level 3.</u> Staff compliance with the code is monitored. The code of conduct must be regularly reviewed.	a	Providing staff with a written code of conduct and briefings does not provide sufficient assurance that the code has been understood and is being followed, therefore compliance spot checks and routine monitoring are conducted. ***We have provided an annual audit check list for the IG Lead which can be used to evidence ongoing monitoring of IG within an organisation. This should be done on a rolling basis and is not designed to be completed in one day – [03].*** <u>Evidence (recommended but not mandatory)</u>: A completed audit sheet or monitoring form, or a report on the outcome of staff compliance checks.
	b	The purpose of providing a code of conduct for staff is to ensure that they use

		personal information in compliance with the law and in line with the expectations of the public. Satisfaction surveys are used to check that patients feel that their confidentiality is respected and that they trust the organisation to hold information securely. ***This can be evidenced through the same "Caring" KLOE surveys that are provided to service users.*** Evidence (recommended but not mandatory): Examples of completed surveys.
	c	[Only required if Attainment Level 3 was achieved in the previous assessment] Policy and law change over time and it is important that the content of code is regularly reviewed and aligned with the latest central guidelines. Evidence (recommended but not mandatory): Minutes/meeting notes where the code has been reviewed during the year including the decisions made and any updates to the guidance.
Resources:	• ***A Staff Confidentiality Code of Conduct Template is available here:*** https://groups.ic.nhs.uk/TheInformationGovernanceKnowledgebase/The%20Information%20Governance%20Knowledgebase/Forms/Code%20of%20Conduct%20Requirement.aspx • [03] ***Annual IG Audit Checklist (Internal)***	
Comments:		

215	**All new processes, services and systems are developed and implemented to comply with information security, information quality and confidentiality and data protection requirements**	
NR: ***This requirement has a 'not relevant' option; however, the requirement is relevant to all Care Providers as they hold service user information, and if new processes, services or systems are introduced there could be an effect on this information. Care Providers must therefore have a procedure in place to reduce the possibility of an adverse impact on service user information.***		
Level 1. There is a documented procedure for ensuring that information security, confidentiality and data protection, and information quality requirements are taken into account before new changes to organisational processes, services or	a	Responsibility has been assigned for documenting a procedure to ensure that new or proposed changes to organisational processes, services or systems are identified. ***There is space in the overarching Information Governance Policy – [01] – to state who has been allocated this responsibility.*** Evidence (recommended but not mandatory): Named individual(s) job description(s), or a signed note or e-mail assigning responsibility.
	b	There is a documented procedure for identifying and assessing new processes, services or systems that might impact on information security, confidentiality and data protection, and information quality. Evidence (recommended but not mandatory): A written document with responsibilities and procedures for deciding whether a privacy impact assessment is required, considering any impact on information quality, reviewing existing security procedures and identifying any new security procedures that may be required.

systems are introduced.		
<u>Level 2.</u> All staff members who may be responsible for introducing changes to processes, services or systems have been effectively informed about the requirement to seek approval. All new implementations follow the documented procedure (or no changes to processes, services or	a	All staff members that are likely to introduce new processes, services or systems are effectively informed about the requirement to obtain approval at the proposal stage of the new process, service or system. Staff might be informed through team meetings, awareness sessions, or staff briefings. ***All new policies/procedures/systems etc. need to be reviewed by the IG Lead who will make a decision whether a Privacy Impact Assessment needs to be made. Assess whether, as part of your induction, you need to include procedures for approving new policy/procedure/processes. If it is only the IG Lead who has the ability to introduce new processes etc. then you do not need to change staff training.*** ***CQC KLOE Safe 3.3 "Do staff receive effective training for safety issues in systems, processes and practices?"*** <u>Evidence (recommended but not mandatory)</u>: Minutes/meeting papers, or notes of team meetings, or staff briefing materials or awareness sessions materials.
	b	All implementations of new processes, services or systems follow the documented procedure, (or no changes to processes, services or systems have been proposed). An appropriate privacy impact assessment is carried out whenever a proposal involves a new use or a significantly changes the way in which personal information is handled.

systems have been proposed). Where the proposed new process, service or system is likely to involve a new use or significantly change the way in which personal data is handled, an appropriate privacy impact assessment is always carried.		***In the instance that you are required to complete a Privacy Impact Assessment [PIA], there is extensive guidance on the Information Commissioner's website. We have provided the link to this guidance in the resource box below.*** Evidence (recommended but not mandatory): Statement that no changes to processes, services or systems have been proposed. Or where necessary, formal risk analysis of Information Governance considerations identified prior to implementation, implementation documentation, and where necessary privacy impact assessment documentation.
Level 3. Compliance with the guidance is monitored by reviewing any new processes, services or systems that have been	a	Specific processes are in place to review proposals and any new processes, services and systems introduced. Where a need for improvement is identified, this is documented within plans and appropriate action taken. Evidence (recommended but not mandatory): Minutes/meeting notes where the new processes, services and systems have been reviewed during the year including the decisions made, and where necessary, action taken to make improvements or any updates to the new processes services or systems.

introduced. Remedial or improvement action is documented and taken where appropriate.	b	Providing staff with written materials or briefings does not provide sufficient assurance that staff understand when to seek approval and that approval is obtained before new processes, services or systems that might impact on information security, confidentiality and data protection, and information quality are introduced. Therefore, compliance spot checks and routine monitoring are conducted. ***We have provided an annual audit check list for the IG Lead which can be used to evidence ongoing monitoring of IG within an organisation. This should be done on a rolling basis and is not designed to be completed in one day – [03]. If staff do not have the authority to make changes to processes etc. then compliance spot checks are not required.*** <u>Evidence (recommended but not mandatory)</u>: Completed monitoring forms, a report on the outcome of staff compliance checks or a review report of requests for approval compared with the new processes, services or systems introduced.
	c	[Only required if Attainment Level 3 was achieved in the previous assessment] Policy and law change over time and it is important that the content of the documented procedure is regularly reviewed and aligned with the latest central guidelines. <u>Evidence (recommended but not mandatory)</u>: Minutes/meeting notes where the procedure has been reviewed during the year including the

		decisions made and any updates to the procedure.
Resources:	• [01] ***Information Governance Policy - Template*** • ***Guidance on completing a Privacy Impact Assessment [PIA] can be found here:*** https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf • [03] ***Annual IG Audit Checklist (Internal)***	
Comments:		

216	**There are appropriate confidentiality audit procedures to monitor access to confidential personal information**	
NR: ***This requirement has a 'not relevant' option; however, all Care Providers create and hold service user records so this requirement will be relevant to you even if these records are paper based.***		
<u>Level 1.</u> There are documented confidentiality audit procedures in place that include the assignment of responsibility for monitoring and auditing access to confidential personal information. The procedures have been	a	Responsibility for documenting confidentiality audit procedures that cover monitoring and auditing access to confidential personal information has been assigned. ***There is space in the overarching Information Governance Policy – [01] – to state who has been allocated this responsibility.*** <u>Evidence (recommended but not mandatory)</u>: Named individual(s) job description, a signed note or e-mail assigning responsibility.
	b	There are documented confidentiality audit procedures that clearly set out responsibilities for monitoring and auditing access to confidential personal information. ***We have provided examples of good confidentiality procedures in our exemplar text – [06]. This must be adapted to reflect your organisation's procedures and processes.*** <u>Evidence (recommended but not mandatory)</u>: Documented confidentiality audit procedures which include the details of the named staff member(s), job role(s).

approved by senior management.	c	The procedures have been approved by senior management. <u>Evidence (recommended but not mandatory)</u>: Sign-off of the procedures document (e.g. the date it was signed-off and by whom).
<u>Level 2.</u> All staff members with the potential to access confidential personal information have been made aware of the procedures. The procedures have been implemented and appropriate action is taken where	a	All staff members with the potential to access confidential personal information have been informed that monitoring and auditing is being carried out, of the need for compliance with confidentiality and security procedures and the sanctions for failure to comply. Staff might be informed through team meetings, awareness sessions, staff briefing materials, or staff might be provided with their own copy of the procedures. ***As part of your staff training procedures you may wish to utilise the Introduction to Information Governance for Staff provided.*** ***There may be some overlap in the evidence for this requirement with 117.*** ***Staff should be informed that monitoring is being carried out. We have provided exemplar text for a Staff Handbook – [2] – which states that this takes place. You should ensure that staff are aware of monitoring through their handbook/intranet/notices, etc.*** <u>Evidence (recommended but not mandatory)</u>: Minutes / meeting notes, or briefing and awareness session materials, or a list of staff signatures that they have read, understood and will comply with the procedures.

confidentiality processes have been breached.	b	The procedures have been effectively implemented and appropriate action is taken where confidentiality processes have been breached or where a near-miss has occurred. Therefore, staff compliance is monitored and there are case reviews if confidentiality processes have been breached or if there has been a near-miss incident. ***We have provided a template Information Security Incident Report Form – [11]. The intention is that these should be easily accessible to staff to complete, similarly to how they would complete a RIDDOR form. Staff should be aware that they should not only report data breaches, but also any near-misses.*** ***As mentioned in the Introduction to Information Governance for Registered Managers, as well as reporting any breaches to the IG Incident Reporting Tool, you should also have an internal disciplinary procedure relating to potential and actual data breaches.*** ***CQC KLOE Well Led 1.4 "Does the service show honesty and transparency from all levels of staff and management following an incident? How is this shared with people using the service and their families in line with the duty of candour, and how does the service support them?"*** Evidence (recommended but not mandatory): Completed monitoring form, or a report on the outcome of staff compliance checks. Where a near-miss has occurred, copies of near-miss reports, lessons learned reports, staff feedback briefings, staff retraining files, or disciplinary

		documents. OR Add a comment that there have been no near-misses. Where a breach has occurred, copies of incident reports, lessons learned reports, staff feedback briefings, staff retraining files or disciplinary documents. OR Add a comment that there have been no breaches.
<u>Level 3.</u> Access to confidential personal information is regularly reviewed. Where necessary, measures are put in place to reduce or eliminate frequently encountered confidentiality events.	a	Access to confidential personal information is subject to regular review, and where necessary, measures are put in place to reduce or eliminate frequently encountered confidentiality events. ***We have provided an annual audit check list for the IG Lead which can be used to evidence ongoing monitoring of IG within an organisation. This should be done on a rolling basis and is not designed to be completed in one day – [03].*** <u>Evidence (recommended but not mandatory)</u>: Minutes / meeting notes where access has been reviewed during the year including the decisions made such as new guidance for staff, improved physical security measures, documented IT system changes (e.g. stronger password formation).
	b	[Only required if Attainment Level 3 was achieved in the previous assessment] Policy and law change over time as do technological developments and it is important that the content of procedures is regularly reviewed, is aligned with the latest central guidelines and takes into account any new systems or processes introduced into the organisation. <u>Evidence (recommended but not mandatory)</u>: Minutes / meeting notes

		where the procedures have been reviewed during the year including the decisions made and any updates to the procedures.
Resources:		• [01] ***Information Governance Policy - Template*** • [02] ***Staff Handbook – Exemplar Texts*** • [03] ***Annual IG Audit Checklist (Internal)*** • [06] ***Confidentiality Policy (including monitoring & auditing access) – Exemplar Texts*** • [11] ***Information Security Incident Report Form - Template***
Comments:		

304	**Monitoring and enforcement processes are in place to ensure NHS national application Smartcard users comply with the terms and conditions of use.**	
NR: ***This requirement can be marked as not relevant for your organisation as long as NHS Smartcards are not used.***		
Level 1. An RA plan or procedure has been developed that sets out how the organisation ensures users are made aware of the Terms and Conditions of Smartcard usage and monitors and enforces compliance. The plan/procedure has been agreed by senior	a	Responsibility has been assigned for developing plan/procedure to monitor and enforce compliance with Terms and Conditions of NHS Smartcard usage. ***There is space in the overarching Information Governance Policy – [01] – to state who has been allocated this responsibility.*** Evidence (recommended but not mandatory): A named individual's job description, a note or e-mail assigning responsibility or the terms of reference of a group.
	b	The plan/procedure identifies how users will be informed of their NHS Smartcard usage responsibilities and how compliance will be monitored. There should be clearly defined actions linked with Human Resource processes for dealing with breaches in the NHS Smartcard usage. ***We have provided a link to the national RA policy template which can be adapted for your organisation's needs. This link is also to the NHS's official guidance on Smartcards.*** Evidence (recommended but not mandatory): Plan/procedure identifies how users will be informed of their NHS Smartcard usage responsibilities. Documented audits of compliance.

management or committee.	c	The plan/procedure has been approved by senior management, an appropriate committee or other established local governance process. <u>Evidence (recommended but not mandatory)</u>: Minutes of meetings, in a document or email or a personal endorsement in writing from an appropriate member of the senior staff. RA Plan/procedure.
<u>Level 2.</u> The plan/procedure has been implemented and all NHS Smartcard users have been effectively informed that NHS Smartcard usage will be monitored, the need for compliance and the sanctions for non-compliance.	a	The plan/procedure for dealing with breaches in NHS Smartcard usage is accessible to users. ***We have provided exemplar text which can be inserted into your staff handbook – [02]*** <u>Evidence (recommended but not mandatory)</u>: Plan/procedure included in a staff handbook or published on the Intranet, or within a procedure folder on the network.
	b	The plan/procedure has been implemented and all NHS Smartcard users including new, temporary and contract staff members are aware that compliance with the terms and conditions of NHS smartcard usage is monitored and of the procedures for breach and disciplinary measures. <u>Evidence (recommended but not mandatory)</u>: Staff briefing and induction materials. Documented audits showing processes for monitoring NHS Smartcard usage and compliance with the NHS Smartcard terms and conditions. Audit report on the outcome of checking that all NHS Smartcard users have

		electronically signed their terms and conditions.
<u>Level 3.</u> Monitoring of NHS Smartcard usage and staff compliance with the terms and conditions is carried out with remedial action taken where non-compliance is identified.	a	NHS Smartcard usage and users' compliance with the terms and conditions is monitored. Where non-compliance is identified, immediate remedial action is taken. ***We have provided an annual audit check list for the IG Lead which can be used to evidence ongoing monitoring of IG within an organisation. This should be done on a rolling basis and is not designed to be completed in one day – [03].*** <u>Evidence (recommended but not mandatory)</u>: A completed monitoring form, or an audit report on the outcome of NHS staff Smartcard usage and compliance checks. HR records, reports to senior management, or in re-training records highlighting any remedial action taken due to non-compliance.
	b	Awareness raising measures are used to ensure users remain compliant and updated with the terms and conditions of NHS Smartcard usage. <u>Evidence (recommended but not mandatory)</u>: Reports, minutes/meeting notes, staff briefing or awareness session materials.
	c	[Only required if Attainment Level 3 was achieved in the previous assessment] It is important that the enforcement and compliance arrangements are

		regularly reviewed to ensure they continue to be effective. Evidence (recommended but not mandatory): Minutes/meeting notes where staff compliance and the enforcement procedures have been reviewed including the decisions made and any updates to the documentation or methods of monitoring.
Resources:		• ***A National Registration Authority and Smartcard policy and official guidance about Smartcards can be found here:*** https://digital.nhs.uk/Registration-Authorities-and-Smartcards • [01] ***Information Governance Policy - Template*** • [02.2] ***Staff Handbook – Exemplar Texts*** • [03] ***Annual IG Audit Checklist (Internal)***
Comments:		

316		**There is an information asset register that includes all key information, software, hardware and services**
Level 1. Responsibility has been assigned to a staff member for compiling information about the organisation's assets and for maintaining the asset register.	a	Responsibility has been assigned for compiling and maintaining an information asset register. ***There is space in the overarching Information Governance Policy – [01] – to state who has been allocated this responsibility.*** Evidence (recommended but not mandatory): A named individual's job description, or a signed note or e-mail assigning responsibility.
Level 2. A list of information assets has been compiled in a register which includes the location and 'owner' for each asset.	a	All information assets (including online / internet facing systems) have been documented in a register that includes relevant details about each asset (i.e. the location of each asset, what type of information, who uses it etc.). ***Note that the IAR is not just about recording pieces of computer equipment, but also a place to note what software is being run i.e. Windows 10 etc. You should also keep a record in the IAR about paper documents. It should record all types of information and how it is stored.*** ***This can be the same IAR as referred to in 202 and 209***

		Evidence (recommended but not mandatory): Documented Information Asset register.
Level 3. The asset register is maintained, reviewed and updated as necessary. Responsibilities and the asset register are regularly reviewed.	a	The asset register is maintained, updated and regularly reviewed, e.g. to ensure that each asset is still required and is still in use or to add new assets to the register. ***We have provided an annual audit check list for the IG Lead which can be used to evidence ongoing monitoring of IG within an organisation. This should be done on a rolling basis and is not designed to be completed in one day – [03].*** Evidence (recommended but not mandatory): Updates to the register or a date and signature indicating it has been reviewed.
	b	[Only required if Attainment Level 3 was achieved in the previous assessment] It is important that the information asset owner carries out their responsibilities appropriately to ensure the currency of the register is maintained and that whenever new assets are introduced to the organisation the register is updated. Evidence (recommended but not mandatory): Minutes/meeting notes where the responsibilities were reviewed during the year including the decisions made and any updates to the register.

Resources:	• [01] ***Information Governance Policy - Template*** • [03] ***Annual IG Audit Checklist (Internal)*** • [07] ***Information Asset Register – Template***
Comments:	

317	**Unauthorised access to the premises, equipment, records and other assets is prevented**	
Level 1. A risk assessment of physical security of the premises has been carried out and staff members have been informed of steps to take in the event of unauthorised access.	a	A risk assessment has been undertaken to identify areas of the premises that are at risk of unauthorised access. This covers the premises as a whole, and takes into account legitimate entry/exit points, areas where forced entry is possible and any unstaffed parts of the premises. ***We have provided a link to a template physical security risk assessment which can be adapted for your organisation. It is likely that your existing security risk assessments will be sufficient evidence for this requirement. The main change is a widening in focus, a lot of previous work has focussed on the security of cash, drugs and people in the organisation. Your risk assessment should now also include the risk to information which is stored, both physical and digital.*** ***CQC KLOE Safe 1.6 "Are people's individual care records, accurate, complete, legible, up to date and securely stored to keep people safe?"*** Evidence (recommended but not mandatory): A documented risk assessment including details of any required improvements.
	b	There is a reporting process and safety measures in place for staff to follow in the event of unauthorised access. ***We have provided exemplar text which may be inserted into your staff handbook – [02].***

		Evidence (recommended but not mandatory): Documented staff guidance.
Level 2. Improvements identified by the risk assessment are being made to secure the premises, equipment, records and other assets and staff.	a	Improvements are being made to secure the premises, equipment, records and other assets. Evidence (recommended but not mandatory): An action plan or allocation of resources or new security equipment (alarms, door locks, etc.) or new ways of working (clear desk, clear screen, etc.) or new archive storage is necessary.
	b	Staff members, including new staff, have been informed about new security measures put in place and the process for reporting unauthorised access through team meetings or awareness sessions or staff briefing or induction materials. Evidence (recommended but not mandatory): Minutes/notes of team meetings, briefing and induction materials.
Level 3. All reasonable steps have been taken to ensure the premises, equipment, records and other assets	a	All improvements identified by the risk assessment have been fully implemented to prevent unauthorised access to the premises, equipment, records and other assets. Evidence (recommended but not mandatory): New security equipment (alarms, door locks, etc.) or new ways of working (clear desk, clear screen, etc.).
	b	Providing staff with guidance and procedures for protecting the premises, equipment, records and other assets does not provide sufficient assurance that the guidance and procedures have been understood and are being

are physically secured. Physical security measures are subject to regular risk assessment.		followed, therefore compliance spot checks and routine monitoring are conducted. ***We have provided an annual audit check list for the IG Lead which can be used to evidence ongoing monitoring of IG within an organisation. This should be done on a rolling basis and is not designed to be completed in one day – [03].*** Evidence (recommended but not mandatory): Completed audit sheets or monitoring forms, or a report on the outcome of staff compliance checks (e.g. review of burglar alarm logs, clear desk procedure, whether windows and doors are locked).
	c	[Only required if Attainment Level 3 was achieved in the previous assessment] It is important that physical security measures are subject to regular risk assessment and updated guidance or procedures are issued to reflect new risks due to new ways of working or the purchase of new equipment. Evidence (recommended but not mandatory): Risk assessments will include checks that security measures are working effectively and that staff are complying with procedures.
Resources:	• ***A template physical security risk assessment can be found here:*** https://groups.ic.nhs.uk/TheInformationGovernanceKnowledgebase/The%20Information%20Governance%20Knowledgebase/Forms/Physical%20Security%20Requirements.aspx • [02.3] ***Staff Handbook – Exemplar Texts***	

	- [03] ***Annual IG Audit Checklist (Internal)*** - ***The ICO has advice on safely storing records here:*** https://ico.org.uk/for-organisations/improve-your-practices/health-sector-resources/
Comments:	

318		The use of mobile computing systems is controlled, monitored and audited to ensure their correct operation and to prevent unauthorised access
NR: This requirement can be marked as not relevant for your organisation if: An assessment of mobile computing use has been conducted and personal information is NOT recorded, viewed, transferred or stored on tapes (including any back-up tapes), PDAs, laptops, mobile phones, memory sticks or equivalent mobile computing equipment. ***If your staff do not use mobile computing equipment this requirement is also not relevant for you.***		
Level 1. There is a record of all staff members that use mobile computing equipment and they have been issued with basic guidelines on the confidentiality and security risks of using mobile computing	a	A record of staff members that use mobile computing equipment has been compiled. ***Although you may like to also have a separate log for this, mobile computing devices can be – and should be - kept track of on your Information Asset Register (IAR). We have provided a template IAR – [07]. Consider carefully who needs access to mobile computing devices in your organisation in order to complete their work, and don't give people access unless it is truly necessary.*** ***Remember that mobile computing devices do not just include mobiles and laptops, but also items such as USB memory sticks and external hard drives.*** ***You can use the same IAR as in 202, 209 & 316.*** Evidence (recommended but not mandatory): One or more documents containing a list of equipment, the date of issue, the security controls applied to it and the member of staff it has been issued to.

equipment.	b	Staff members are actively encouraged to use the equipment responsibly to prevent unauthorised access and they have been provided with basic guidance on the risks that may exist and the precautions they should take to protect equipment and the information it contains. *We have provided an assignment of mobile computing equipment form [12] for staff that have been given a mobile computing device to complete. We have also provided template guidance to staff on the correct use of business mobile devices [13].* *The IG Toolkit recommends that Good Practice Guidance for staff should include advice about:* *a) "Locking the machine up overnight, or removing the hard-drive or memory card (where possible) if the machine cannot be locked away.* *b) Not leaving the system unattended, e.g. on the seat of a car.* *c) Using secure passwords to prevent unauthorised access to information stored on the computer.* *d) Ensuring password security.* *e) Reporting lost or stolen equipment promptly."* Evidence (recommended but not mandatory): Staff briefing materials and a signed declaration from the user (that they will comply with conditions of use) on allocation of the equipment.

Level 2. Procedures and processes to control the use of mobile computing systems have been implemented, and there is comprehensive guidance for staff on the use of mobile computing systems.	a	There are procedures to ensure that the issue of mobile computing equipment is controlled and appropriate. ***See the example texts provided.*** Evidence (recommended but not mandatory): Documented evidence that the equipment has only been issued to appropriate staff (e.g. in records of allocation of equipment and in staff declaration forms).
	b	Access to internal IT systems is controlled, and there are robust authentication procedures in place for all staff having remote access to systems. ***If no one has remote access to your system you can state this in the comment box for this requirement.*** Evidence (recommended but not mandatory): Documented evidence that the authentication of remote users is to a greater level of assurance than internal users.
	c	There is comprehensive guidance for staff on the correct operation of mobile computing equipment and the prevention of unauthorised access. Staff members have been informed of the guidance and in particular of their own responsibilities for appropriately accessing and using the equipment. Staff may be informed through team meetings, or awareness sessions or staff briefing materials. ***See the example texts provided.***

		Evidence (recommended but not mandatory): Documented guidance for staff. Minutes/meeting notes of team meetings or briefing materials used in awareness sessions.
Level 3. The use of mobile computing systems is monitored and audited. The procedures, processes and staff guidance are regularly reviewed.	a	Providing staff with guidance for mobile computing systems does not provide sufficient assurance that the guidance has been understood and is being followed, therefore compliance spot checks and routine monitoring are conducted. ***We have provided an annual audit check list for the IG Lead which can be used to evidence ongoing monitoring of IG within an organisation. This should be done on a rolling basis and is not designed to be completed in one day – [03].*** Evidence (recommended but not mandatory): Completed audit sheet or monitoring form, or a report on the outcome of staff compliance checks.
	b	Audits are carried out to ensure that equipment is appropriately allocated. This might be done by reviewing the records created when equipment is allocated to ensure that the reason for the allocation is still valid. Evidence (recommended but not mandatory): A completed checklist or report on the outcome of the audit.
	c	[Only required if Attainment Level 3 was achieved in the previous assessment] The robustness of security and access controls may change over time, and it is important that procedures, processes and staff guidance take account of any

		changes made to the technical access controls in systems. ***As technology develops and the amount used in your organisation changes, it is important that information governance is considered when implementing and procuring new technology.*** Evidence (recommended but not mandatory): Minutes/meeting notes where the documentation has been reviewed during the year including the decisions made and any updates.
Resources:	• [03] ***Annual IG Audit Checklist (Internal)*** • [07] ***Information Asset Register - Template*** • [12] ***Assignment of Mobile Computing Equipment Form – Template*** • [13] ***Staff Guidelines: Using Mobile Computing Equipment - Template***	
Comments:		

319	**There are documented plans and procedures to support business continuity in the event of power failures, system failures, natural disasters and other disruptions**	
Level 1. There has been an assessment of the risks to all systems where information critical to the running of the organisation is held.	a	There has been an assessment of the risks to all systems where information critical to the running of the organisation is held which has been documented. ***We have provided a Business Impact Analysis document [14]. A physical security risk assessment has already been completed as part of requirement 317.*** ***It is important to consider what might cause any information loss as it might be quite different for paper based, computer based or cloud based information. Some organisations will only have to worry about hard copy information, some only with digitally stored data and many with a combination of the two.*** Evidence (recommended but not mandatory): A business impact analysis document.
Level 2. There is a business continuity plan that has been approved by	a	There is an approved business continuity plan in place, which has been approved by senior management. ***We have provided exemplar text which can be inserted into your Emergency and Business Continuity Plan [15].***

senior management. All staff are aware of their roles and responsibilities		<u>Evidence (recommended but not mandatory)</u>: Documented business continuity plan. Approval may be in the minutes/notes of meetings, in a document or email or a personal endorsement in writing from an appropriate member of the senior staff.
	b	All relevant staff are made aware of the business continuity plan and any implications for their role. <u>Evidence (recommended but not mandatory)</u>: Notes/minutes from team meetings, or briefing materials used in awareness sessions.
<u>Level 3.</u> There is an approved business continuity plan in place which has been tested. The business continuity plan is regularly reviewed.	a	Annual testing is carried out to ensure that business continuity plans are effective and robust and will work in an operational environment. ***We have provided an annual audit check list for the IG Lead which can be used to evidence ongoing monitoring of IG within an organisation. This should be done on a rolling basis and is not designed to be completed in one day – [03].*** <u>Evidence (recommended but not mandatory)</u>: Documentation for testing processes (e.g. a table top exercise, simulation, or walk through exercise), or minutes/notes of discussions detailing agreed tests.
	b	[Only required if Attainment Level 3 was achieved in the previous assessment] It is important that business continuity plans are regularly reviewed and updated (and in particular when new threats are identified) so that the

		organisation has the necessary assurances that plans are capable of being executed effectively. <u>Evidence (recommended but not mandatory)</u>: Minutes/meeting notes where the plan has been reviewed during the year including the decisions made and any updates to the plan.
Resources:	• [03] ***Annual IG Audit Checklist (Internal)*** • [14] ***Business Impact Analysis Document - Template*** • [15] ***Emergency & Business Continuity Plan – Exemplar Text***	
Comments:		

320	There are documented incident management and reporting procedures	
[redacted]		[redacted]
Level 1. Responsibility for leading on the management and reporting of information incidents has been assigned to an appropriate member of staff.	a	Responsibility for leading on the management and reporting of information incidents has been assigned to an appropriate member of staff. Where necessary and available, support is obtained from the commissioning organisation. ***There is space in the overarching Information Governance Policy – [01] – to state who has been allocated this responsibility.*** Evidence (recommended but not mandatory): A named individual's job description, or a signed note or e-mail assigning responsibility. Evidence of commissioning organisation support if required may be in email communications, or in a formal SLA.
Level 2. Incident management and reporting procedures have been implemented and staff have been	a	There are incident management and reporting procedures. ***We have provided template Data Security Breach Procedures [16] for you and a template Information Security Incident Report Form [11].*** ***Note that data security breaches should be considered as a disciplinary offence and your staff should be informed of this.*** ***Although cyber security is not the only form of security measure you will***

informed of how to report incidents and near-misses.		***follow to protect information, we have provided a link to a detailed guidance which is aimed at small businesses on how to improve cyber security within the resources.*** Evidence (recommended but not mandatory): Documented procedures and a template incident reporting form for staff.
	b	Staff members have been informed of the incident reporting procedures and in particular of their own responsibilities for reporting incidents and near-misses. ***All staff have a responsibility for information governance and security and so should all receive training on what to do in the case of an incident. It is likely that the training and contract changes you made to fulfil requirements 116 and 117 will cover you for this requirement as well.*** Evidence (recommended but not mandatory): Minutes/notes of team meetings, or briefing materials used in awareness sessions.
	c	Any information incidents that arise are reported to the senior management team and where necessary to the commissioning organisation and external parties. Reports include details of investigations or action taken and detail any possible countermeasures. ***There is extensive guidance on incident reporting in the IG Toolkit Guidance for this requirement and there is a link to the IG Incident Reporting Tool User Guide in the resource box below. The Information Governance Alliance have also provided guidance on reporting IG Incidents and this is linked in***

		the resource box below. Evidence (recommended but not mandatory): Completed incident reporting forms and reports made to senior management and where necessary to the commissioning organisation, the Information Commissioner, insurers, or the police. OR If there have been no breaches, state this in the comments section or add the words 'not relevant'.
Level 3. Incident reporting and management procedures are being followed and appropriate action is taken in the event of an incident or near-miss. Incident reporting and management procedures are regularly reviewed.	a	Providing staff with procedures for reporting incidents does not provide sufficient assurance that the procedures have been understood and are being followed. Therefore, compliance checks and routine monitoring are conducted. ***We have provided an annual audit check list for the IG Lead which can be used to evidence ongoing monitoring of IG within an organisation. This should be done on a rolling basis and is not designed to be completed in one day – [03].*** Evidence (recommended but not mandatory): A completed audit sheet or monitoring form, or a report on the outcome of staff compliance checks.
	b	Information incidents and near-misses are appropriately discussed with staff and where necessary, retraining is carried out or new security measures are implemented. Evidence (recommended but not mandatory): Minutes/meeting notes or lessons learned documents. Where necessary, training materials or evidence of new measures put in place.

	c	[Only required if Attainment Level 3 was achieved in the previous assessment] No matter how good existing procedures are weaknesses will always become apparent. New threats and new systems or ways of working will expose these weaknesses and users on the ground are normally the first to identify them. Therefore, staff should be encouraged to report anything they feel threatens security, and this approach needs to be adopted during induction training. Evidence (recommended but not mandatory): Staff briefing materials, or incident report forms, or induction materials or new security measures.
Resources:		• [01] ***Information Governance Policy - Template*** • [02.4] ***Staff Handbook – Exemplar Texts*** • [03] ***Annual IG Audit Checklist (Internal)*** • [11] ***Information Security Incident Report Form - Template*** • [16] ***Data Security Breach Procedures – Exemplar Text*** • ***Information on how to protect your organisation from cyber-attacks is available here:*** https://www.gov.uk/government/publications/cyber-security-what-small-businesses-need-to-know • ***Further information about how small businesses can be cyber secure can be found here:*** https://www.gov.uk/government/publications/cyber-security-what-small-businesses-need-to-know • ***Further information about Incident Reporting can be found here:*** https://www.igt.hscic.gov.uk/resources/HSCIC%20SIRI%20Reporting%20and%20Checklist%20Guidance.pdf • ***Further information about Incident Reporting can also be found here:***

	https://groups.ic.nhs.uk/TheInformationGovernanceKnowledgebase/The%20Information%20Governance%20Knowledgebase/HSCIC%20SIRI%20Reporting%20and%20Checklist%20Guidance_V5%201%20290515_Final_Publish.pdf
Comments:	

321		**There are appropriate procedures in place to manage access to computer-based information systems**
Level 1. There is documented procedure for allocating and managing access to computer-based information systems.	a	A procedure has been documented that sets out how access to computer-based information systems will be allocated and managed. ***It is important to consider who in your organisation has access to what information and why. Do all staff have access to the computer? Is this something that they need to have? Or do some people only need to have access to patient care plans, or some to only have access to information so that they can complete payroll?*** ***Confidential and sensitive information must only be accessed by people who need to have access to it, this is not decided on a hierarchical basis. There is more information in the Introduction to Information Governance for Registered Managers on the difference between confidential and sensitive personal data.*** ***We have provided Guidelines on the Appropriate Use of Computer Systems for Staff [18] and also template Access Management procedures [17] which can be adapted and act as suggestions of good practise for your organisation. There is a template Access Management Log for you to keep track of user access – for larger organisations with an ICT Supplier or support team, they may be able to do this for you.*** ***We have provided exemplar texts which can be inserted into your staff***

		handbook [02]. ***There may well be some overlap with requirement 216 in the evidence for this requirement.*** <u>Evidence (recommended but not mandatory)</u>: Documented procedure.
	b	Responsibility for allocating and removing access rights to the system has been assigned. <u>Evidence (recommended but not mandatory)</u>: A named individual's job description, or a signed and dated note or e-mail assigning responsibility.
	c	The procedure has been approved by a senior member of staff. <u>Evidence (recommended but not mandatory)</u>: Minutes of meetings, or in a document or email or a personal endorsement in writing from an appropriate member of the senior staff.
<u>Level 2.</u> The procedures have been implemented and access to the computer-based information	a	Access to information assets is only possible for individuals who have been duly authorised. <u>Evidence (recommended but not mandatory)</u>: Access management procedures such as user registration and deregistration including temporary access, (e.g. for contractors and locums), signatures/electronic evidence of authorisations, the disabling and erasure of unused accounts.
	b	All staff members have been informed of the procedures and in particular of their own responsibilities for accessing and using the system in accordance with the procedures. Staff may be informed through team meetings, or

systems is restricted to authorised users only and all staff are aware of their responsibility to appropriately use the system.		awareness sessions or staff briefing materials. Evidence (recommended but not mandatory): Minutes/meeting notes of team meetings or briefing materials or materials used in awareness sessions.
Level 3. Compliance with the access management procedures is monitored. The procedure is regularly reviewed.	a	A process has been developed to monitor compliance with the access management procedures. ***We have provided an annual audit check list for the IG Lead which can be used to evidence ongoing monitoring of IG within an organisation. This should be done on a rolling basis and is not designed to be completed in one day – [03].*** Evidence (recommended but not mandatory): Completed audit sheets or monitoring forms, or a report on the outcome of staff compliance checks.
	b	Access requirements are routinely reviewed to ensure that user access privileges remain appropriate, and where access is no longer required, it is disabled or revoked.

		Evidence (recommended but not mandatory): Audit sheets (e.g. checking what access people have), or reports from monitoring software, or minutes/notes from review meetings, or auditable log files, or comparison of deregistration against leavers' records.
	c	[Only required if Attainment Level 3 was achieved in the previous assessment] The robustness of security and access controls may change over time, and it is important that the procedure takes account of any changes made to the technical access controls in systems by system suppliers. Evidence (recommended but not mandatory): Minutes/meeting notes where the procedure has been reviewed during the year including the decisions made and any updates.
Resources:	• [01] ***Information Governance Policy - Template*** • [02.5] ***Staff Handbook – Exemplar Texts*** • [03] ***Annual IG Audit Checklist (Internal)*** • [17] ***Access Control Procedures – Template*** • [18] ***Staff Guidelines on The Appropriate Use of Computer Systems – Template***	
Comments:		

322		**All transfers of hardcopy and digital personal and sensitive information have been identified, mapped and risk assessed; technical and organisational measures adequately secure these transfers**
<u>Level 1.</u> Transfers of personal and sensitive information to and from the organisation have been identified and there is a documented procedure for the secure transfer and receipt of personal and sensitive information, which has been approved by senior management.	a	Routine flows of personal and sensitive information (hardcopy and digital) to and from the organisation have been identified and recorded. ***NHS Digital has extensive advice on how to create mapping documents, we have provided the link in the resources section below.*** ***Note that there may be some overlap with requirement 202 for the evidence required for this.*** ***CQC KLOE Well-Led 5.2 "Does the service share appropriate information and assessments with other relevant agencies for the benefit of people who use the service?"*** <u>Evidence (recommended but not mandatory)</u>: Mapping documents showing with whom, where and how information is exchanged.
	b	There is a documented procedure for the secure transfer and receipt of personal and sensitive information, which has been approved by a senior member of staff. ***We have provided a template information handling policy and procedures [19].***

		Evidence (recommended but not mandatory): Documented procedure with senior management sign off (e.g. signature on the document).
Level 2. All risks areas are appropriately reported and all staff members who transfer and receive personal information have been made aware of the appropriate methods for secure transfer and receipt of personal and sensitive information.	a	All information flows have been identified and recorded, and risks in transfer methods have been assessed. Where necessary remedial action has been taken where a significant risk is revealed including informing the commissioning organisation where necessary. Evidence (recommended but not mandatory): A documented report detailing all information flows, recorded risks and actions taken to secure the information.
	b	Risks to information need to be considered at an appropriately high level in the organisation and therefore there is a structured method of reporting information risks, including where necessary, informing the commissioning organisation. Evidence (recommended but not mandatory): Senior staff sign off of risk reports, minutes of meetings and where necessary, reports for the commissioning organisation.
	c	Relevant staff members have been effectively informed of the secure transfer and receipt requirements for personal and sensitive information. ***We have provided exemplar text to be inserted into the staff handbook [02].*** Evidence (recommended but not mandatory): An acceptable use policy for

		email and internet use, data handling procedures, safe haven procedures, training materials or other staff guidance supported by evidence of staff awareness of and compliance with such documentation. These may be in a single document for convenience.
Level 3. Personal and sensitive information flows are regularly reviewed and where necessary records are updated to reflect any changes in flow methods, locations or data items. Compliance with the procedures is monitored to ensure that information is handled and transferred	a	Flows of personal and sensitive information are regularly reviewed and records are updated to reflect any changes in flow methods, locations or data items. ***We have provided an annual audit check list for the IG Lead which can be used to evidence ongoing monitoring of IG within an organisation. This should be done on a rolling basis and is not designed to be completed in one day – [03].*** Evidence (recommended but not mandatory): Updated records or the issue of new procedures for staff.
	b	Providing staff with procedures does not provide sufficient assurance that the procedures have been understood and are being followed, therefore compliance spot checks and routine monitoring is conducted. Evidence (recommended but not mandatory): Completed audit sheets or monitoring forms, or a report on the outcome of staff compliance checks.
	c	[Only required if Attainment Level 3 was achieved in the previous assessment] Policy and law change over time as do technological advances and it is important that transfers of information are regularly reviewed and the

appropriately. The flows and transfer methods of person identifiable and sensitive information are regularly reviewed and the technical and organisational measures are updated, where necessary, to reflect any changes.		secure transfer procedure remains aligned with the latest central guidelines. Evidence (recommended but not mandatory): Minutes/meeting notes where the controls and procedures have been reviewed including the decisions made and any updates to the controls or procedures.
Resources:	• ***Further information about Information Flows and Mapping can be found here:*** • https://www.igt.hscic.gov.uk/datamappingguidance.aspx • ***There is more information available about information handling, flows and mapping here:*** • https://groups.ic.nhs.uk/TheInformationGovernanceKnowledgebase/The%20Information%20Governance%20Knowledgebase/Forms/Information%20Asset%20Register.aspx	

	- [02.6] ***Staff Handbook – Exemplar Texts*** - [03] ***Annual IG Audit Checklist (Internal)*** - [19] ***Information Handling Policy and Procedures - Template***
Comments:	

<table>
<tr><th>325</th><th colspan="2">Policy and procedures are in place to ensure that Information Communication Technology (ICT) networks operate securely</th></tr>
<tr><td colspan="3">NR: *This requirement can be marked as not relevant for your organisation if:* ICT networks are not controlled by the organisation.
An ICT network is when you have a set of 2 or more computers which are linked together and share information and resources. If you do not have a network then this requirement is not relevant for you.</td></tr>
<tr><td>Level 1.
Responsibility for network security has been assigned to an individual who undertakes reviews of information security risks. Mitigating controls and procedures have been identified and documented.</td><td>a</td><td>Responsibility has been assigned for documenting a network security policy for each ICT network and for undertaking information security reviews.
If you have an ICT network, someone within your organisation should be responsible for its running. If you use an external ICT supplier or support, then make sure that your contracts with them ensure the security of your network and liaise with them on how they and you will react should something happen to the network.
We have provided a template Network Security Policy which can be adapted for your organisation [20].
Evidence (recommended but not mandatory): Named individual(s) job description(s), or a signed note or e-mail assigning responsibility.
Documented ICT network security policy /policies.</td></tr>
<tr><td></td><td>b</td><td>Reviews of information security risk in relation to ICT networks are undertaken, and appropriate controls and procedures to mitigate any risks are documented in the network security policy/policies.</td></tr>
</table>

		In smaller organisations where you do not have an internal IT Support team or IT expert, it is very important that you work with an external IT Supplier/Support who can help you and provide advice on any risks that might affect your organisation. Your IT Supplier/Support may also be able to take on a lot of the monitoring and auditing of systems which will reduce the burden of access management and other policies/procedures on you personally. Evidence (recommended but not mandatory): Risk review documentation, ICT network security policies, documented procedures.
	c	Network security controls and procedures that mitigate against risks have been signed off by a senior member of the organisation. Evidence (recommended but not mandatory): Sign off documented on the ICT network security policy document(s) (for example - the date of sign-off and by whom).
Level 2. The approved controls and procedures for network security in respect of all ICT networks controlled by the	a	The identified controls and procedures have been implemented in respect of all networks in accordance with the ICT network security policy/policies. Evidence (recommended but not mandatory): A single document which identifies the controls applied, such as network capacity planning, network security, reliable firewalls, gateways and domains and file storage facilities supporting individual and group access.
	b	The documented and approved controls and procedures have been made available to appropriate staff who have been informed of their responsibilities to maintain network security by complying with them.

organisation have been implemented.		Informing staff might be done through team meetings, staff briefings, awareness sessions and by IT user induction training. <u>Evidence (recommended but not mandatory)</u>: Minutes/meeting notes, briefing and awareness session materials or a list of staff signatures that they have read, understood and will comply with the procedures.
<u>Level 3.</u> Compliance with the implemented ICT network security controls and procedures is monitored, and remedial or improvement action is promptly taken. Regular security risk reviews and assurance reports are provided to senior	a	Compliance with the ICT network security policy/policies is monitored and where necessary, prompt remedial or improvement is action taken. ***It may be that network security is monitored by your IT contractor or supplier. They may be able to provide these reports and tests as part of your service.*** <u>Evidence (recommended but not mandatory)</u>: Reports of the outcome of staff spot checks, monitoring software, results from audits (including technical) and penetration testing, and checks of system documentation and functionality. Implementation of new controls, reconfigured controls, or new guidance for staff.
	b	Regular security risk reviews and assurance reports are provided to senior management. ***We have provided an annual audit check list for the IG Lead which can be used to evidence ongoing monitoring of IG within an organisation. This should be done on a rolling basis and is not designed to be completed in one day – [03].***

management.		Evidence (recommended but not mandatory): Formal reports, briefing notes, or minutes of meetings where network security was discussed.
	c	[Only required if Attainment Level 3 was achieved in the previous assessment] Existing policy and associated controls and procedures must be regularly reviewed to ensure that ICT networks continue to operate securely. Evidence (recommended but not mandatory): Minutes/meeting notes where the controls and procedures have been reviewed including the decisions made and any updates to the controls or procedures.
Resources:		• [01] ***Information Governance Policy – Template*** • [03] ***Annual IG Audit Checklist (Internal)*** • [07] ***Information Asset Register - Template*** • [20] ***ICT Network Security Policy – Template***
Comments:		

<table>
<tr><th>412</th><th colspan="2">Procedures are in place to ensure the accuracy of service user information on all systems and /or records that support the provision of care, support and advisory services</th></tr>
<tr><td colspan="3">NR: *This requirement has a ‘not relevant’ option; however, all Care Providers create and hold service user records so this requirement will be relevant to you.*</td></tr>
<tr><td rowspan="2">Level 1.
There are documented and approved procedures to ensure the accuracy of service user information on all systems and/or records that support the provision of care, support and advisory services.</td><td>a</td><td>Responsibility for developing and implementing procedures for ensuring the accuracy of service user information on all systems and/or records that support the provision of care, support and advisory services has been assigned.
There is space in the overarching Information Governance Policy – [01] – to state who has been allocated this responsibility.
Evidence (recommended but not mandatory): Named individual(s) job description(s), or a signed note or e-mail assigning responsibility.</td></tr>
<tr><td>b</td><td>The procedures have been documented.
These procedures are going to be the same as those which are likely to already exist in your organisation as good governance and record keeping is detailed in the Health and Social Care Act 2008 (Regulated Activities), Regulations 2014: Regulation 17. CQC guidance on this regulation is linked in the resource box below.
CQC KLOE Safe 1.6 “Are people’s individual care records, accurate, complete, legible, up to date and securely stored to keep people safe?”
Evidence (recommended but not mandatory): One or more documented</td></tr>
</table>

		procedures (for example, an overall data quality procedure incorporating all aspects of data collection, validation and correction of errors, or in a number of separate procedure documents covering these areas).
	c	The procedures have been approved by a senior staff member Evidence (recommended but not mandatory): Minutes/meeting notes, in a document or email, or a personal endorsement in writing.
Level 2. Data collection and validation activities are regularly monitored. All staff collecting and recording data are effectively trained to do so and dedicated staff take appropriate action where errors and omissions are identified.	a	Data collection and validation activities are regularly monitored and data quality reports routinely considered by senior management. ***The audits which you perform in order to evidence to CQC that clinical care plans are reviewed regularly and are accurate are sufficient.*** Evidence (recommended but not mandatory): Documented Data Quality Reports
	b	Procedures have been made accessible to all staff involved in data collection activities. ***We have provided exemplar text to insert into your staff handbook [02].*** Evidence (recommended but not mandatory): A list of staff signatures confirming that they have read and understood the procedures.
	c	All staff entering data are effectively trained to accurately collect and record service user information, check the information with an appropriate source and report errors or omissions.

		Evidence (recommended but not mandatory): Training materials, training attendance records, or staff briefings. Errors/omission logs.
	d	Dedicated staff carry out activity reconciliations between the service user record and data held on systems that support the provision of care, support and advisory services and correct errors and omissions. Evidence (recommended but not mandatory): Job descriptions of dedicated staff that carry out activity reconciliations. Audit or system reports showing that the databases have been synchronised, system reports showing errors/omissions have been corrected, or regular data quality reports.
Level 3. Regular audits and reviews are carried out to monitor the effectiveness of data collection and validation activities.	a	Providing staff with training does not provide sufficient assurance that the procedures have been understood and are being followed, therefore data collection and validation activities are audited and compliance spot checks are conducted. ***We have provided an annual audit check list for the IG Lead which can be used to evidence ongoing monitoring of IG within an organisation. This should be done on a rolling basis and is not designed to be completed in one day – [03].*** Evidence (recommended but not mandatory): Documented audit and completed monitoring forms or a report on the outcome of staff compliance checks.

	b	[Only required if Attainment Level 3 was achieved in the previous assessment] It is important that the procedures are regularly reviewed and aligned with the latest central guidance. Training materials should be regularly reviewed in line with updates to systems or new guidance. Evidence (recommended but not mandatory): Minutes/meeting notes where the procedures have been reviewed during the year including the decisions made and any updates to the procedures and copies of updated training materials, staff guidance or hand-outs.
Resources:	• [01] ***Information Governance Policy – Template*** • [02.7] ***Staff Handbook – Exemplar Text*** • [03] ***Annual IG Audit Checklist (Internal)*** • [21] ***Records Management Policy & Procedures – Template*** • http://www.cqc.org.uk/content/regulation-17-good-governance	
Comments:		

Resources

Contents

For your information: 3

[01] Information Governance Policy 4

[02] Staff Handbook...13

[03] Annual IG Audit Checklist (Internal)..18

[04] Staff Contracts...22

[05] Third Party Contract – Confidentiality Agreement...........................23

[06] Confidentiality Policy (including monitoring & auditing access)...27

[07] Information Asset Register 33

[08] General Consent on Admission Form..36

[09] Service User Handbook...37

[10] Service User Leaflet 40

[11] Information Security Incident Report Form 43

[12] Assignment of Mobile Computing Equipment Form 45

[13] Staff Guidelines: Using Mobile Computing Equipment 46

[14] Business Impact Analysis Document...51

[15] Emergency & Business Continuity Plan.......................................54

[16] Data Security Breach Procedures...57

[17] Access Control policy & procedures & Access Management Log .59

Access Management Log 64

[18] Staff Guidelines on The Appropriate Use of Computer Systems .. 65

[19] Information Handling Policy Procedures..................................... 69

[20] ICT Network Security Policy - Template 74

[21] Records Management Policy & Procedures - Template 81

For your information:

The following templates and exemplar texts have been provided to help you attain Information Governance (IG) Toolkit compliance. Some may not be relevant for your organisation, in which case you do not have to use them. Equally, you may already have policies and procedures in place which contain the same information but under a different name or in different words. This is fine.

Some texts may contain sections which are not relevant to your organisation, these can be altered or deleted as needed – for example, there is no need to assign responsibility for NHS Smartcard usage in [01] Information Governance Policy if you do not have Smartcards.

All text which is bolded and in square brackets, *i.e.* **[text]**, are to indicate where you should insert information specific to your organisation within the templates. That is not to say, however, that this is the only place which can be edited.

These templates are intended to be **adapted** to your needs.

[01] Information Governance Policy - Template

Information Governance Policy

1. Summary

1.1. Information is a vital asset, both in terms of the clinical management of individual service users and the efficient management of services and resources. It plays a key part in clinical governance, service planning, performance management and compliance with Care Quality Commission (CQC) regulations.

1.2. It is of paramount importance to ensure that information is efficiently managed, and that appropriate policies, procedures and management accountability and structures provide a robust governance framework for information management.

2. Principles

2.1. **[Insert organisation name]** (hereafter referred to as "us", "we", or "our") recognises the need for an appropriate balance between openness and confidentiality in the management and use of information *i.e.* Information Governance (IG).

2.2. The importance of safeguarding both personal information about service users and staff and commercially sensitive information is paramount; however, we emphasise the importance of sharing service user information with other Health & Social Care organisations and other agencies in a controlled manner consistent with the interests of the service user and, in some circumstances, the public interest. In all instances, the focus remains on the safeguarding and sharing of personal, sensitive and confidential information in line with legal and regulatory requirements.

2.3. We believe that accurate, timely and relevant information is essential to deliver the highest quality Health & Social Care. As such it is the responsibility of all staff and managers to ensure and promote the quality of information and to actively use information in decision making processes.

3. Our approach to Information Governance (IG):

3.1. We undertake to implement IG effectively and will ensure the following:

i. Information will be protected against unauthorised access;
ii. Confidentiality of information will be assured;
iii. Integrity of information will be maintained;
iv. Information will be supported by the highest quality data;
v. Regulatory and legislative requirements will be met;
vi. Business continuity plans will be produced, maintained and tested;
vii. IG training will be available to all staff as necessary to their role;
viii. All breaches of confidentiality and information security, actual or suspected, will be reported and investigated.

4. Procedures.

[The procedures & policies may have different names in your organisation. You should update the following to reflect this.]

Resources

4.1. This IG policy is underpinned by the following policies and procedures:

i. Record Keeping policy & procedure **[Insert Policy Number]** that set outs how service user records will be created, used, stored and disposed of;

ii. Access policy & procedure [Insert Policy Number] that sets out procedures for the management of access to confidential information; [Note that this policy should cover hard-copy (paper) based information and, if applicable in your organisation, digital information.]

iii. Monitoring of Business Communications policy & procedure **[Insert Policy Number]** that sets out procedures around the transfer of confidential information;

iv. Data Security Breach policy & procedure **[Insert Policy Number]** that sets out the procedures for managing and reporting information incidents;

v. Business continuity plan that sets out the procedures in the event of a security failure or disaster affecting computer systems;

vi. Staff Confidentiality Code of Conduct **[Insert policy number]** that provides staff with clear guidance on the disclosure of personal information.

4.2. There are 4 key interlinked strands to the IG policy:

i. Openness

ii. Legal compliance

iii. Information security

iv. Quality assurance

5. Openness

5.1. We will be open and transparent with service users and those who lawfully act on their behalf in relation to their care and treatment. We will adhere to our responsibilities as outlined in the Health and Social Care Act 2008 (Regulated Activities), Regulations 2014: Regulation 20: Duty of candour.

5.2. Service users should have ready access to information relating to their own health care, their options for treatment and their rights as service users.

5.3. There are clear procedures and arrangements for handling queries from service users and the public.

5.4. There are clear procedures and arrangements for liaison with the press and broadcasting media.

6. Legal Compliance

6.1. All identifiable personal information relating to service users is confidential.

6.2. All identifiable personal information relating to staff is confidential except where national policy on accountability and openness requires otherwise.

6.3. We will establish and maintain policies to ensure compliance with the Data Protection Act 1998, Human Rights Act 1998 and the Common Law Duty of Confidentiality.

6.4. We will establish and maintain policies for the controlled and appropriate sharing of service user and staff information with other agencies, taking account of relevant legislation (*e.g.* Health and Social Care Act 2012, Crime and Disorder Act 1998, etc.).

6.5. We will undertake or commission annual assessments and audits of our compliance with legal requirements.

7. <u>Information Security</u>

7.1. We will establish and maintain policies for the effective and secure management of its information assets and resources.

7.2. We will undertake or commission annual assessments and audits of our information arrangements.

7.3. We will promote effective confidentiality, security and information sharing practices to our staff through policies, procedures and training.

7.4. We will establish and maintain incident reporting procedures and will monitor and investigate all reported instances of actual or potential breaches of confidentiality and security.

8. <u>Information Quality Assurance</u>

8.1. We will establish and maintain policies and procedures for information quality assurance and the effective management of records.

8.2. We will undertake or commission annual assessments and audits of our information quality and records management arrangements.

8.3. Senior staff are expected to take ownership of, and seek to improve, the quality of information within our service.

8.4. Wherever possible, information quality should be assured at the point of collection. For example, when employing new staff all details taken should be thoroughly checked to ensure accuracy.

8.5. Data will be stored and recorded in line with Data Standards legislation – *i.e.* the Data Protection Act 1998.

8.6. We will promote information quality and effective records management through policies, procedures/user manuals and training.

9. Responsibilities

9.1. The designated Information Governance Lead for the organisation is **[insert IG Lead name here]** and, in their absence, their Deputy **[Insert Deputy Name Here, if applicable]**.

The key responsibilities of the lead are:

i. To define **[insert organisation name]**'s policy in respect of IG and ensuring that sufficient resources are provided to support the requirements of the policy.

ii. To complete the NHS Information Governance Toolkit and maintain compliance *i.e.* Level 2 or above in all requirements.

iii. Developing and implementing IG procedures and processes for the organisation; **[those required to complete the IG Toolkit have been provided for you]**

iv. Raising awareness and providing advice and guidelines about IG to all staff;

v. Ensuring that any training made available is taken up;

vi. Coordinating the activities of any other staff given data protection, confidentiality, information quality, records management and Freedom of Information responsibilities;

vii. Ensuring that service user data is kept secure and accurate and that all data flows, internal and external, comply with the Caldicott Principles;

viii. Monitoring information handling in the organisation to ensure compliance with law, guidance and the organisation's procedures;

ix. Ensuring service users are appropriately informed about the organisation's information handling activities;

x. Overseeing changes to systems and processes;

xi. Incident reporting. Any/all breaches will be appropriately dealt with, investigated and reported to NHS Digital via the IG Toolkit website (https://www.igt.hscic.gov.uk/).

xii. Ensuring that sufficient resources are provided to support the effective implementation of IG in order to ensure compliance with the law, professional codes of conduct and the NHS Information Governance assurance framework.

[You need to state who is responsible for the following within your organisation, if they are not applicable then please delete.]

9.2. **[insert job title here]**, is responsible for the Information Assets Register – this is the list of all devices and computer equipment in the organisation including who is responsible for it and what security has been applied to it, *i.e.* passwords or encryption, it also contains storage areas and protections for non-digital records.

9.3. **[insert job title here]**, is responsible for monitoring and enforcing compliance with the terms and conditions of NHS Smartcard usage (the Registration Authority manager).

9.4. **[insert job title here]**, is responsible for reviewing transfers of personal information outside of the UK. **[Note that if this is applicable it may be the responsibility of the same person who maintains the IAR].**

9.5. **[insert job title here]**, is responsible for the ICT services including access rights to computer based systems.

9.6. All staff, whether permanent, temporary or contracted, and contractors are responsible for ensuring that they are aware of and comply with the requirements of this policy and the procedures and guidelines produced to support it.

10. Policy Approval

10.1. **[Insert organisation name]** acknowledges that information is a valuable asset, therefore it is wholly in our interest to ensure that the information we hold, in whatever form, is appropriately governed, protecting the interest of all stakeholders.

10.2. This policy, and its supporting standards and work instruction, are fully endorsed by **[insert either the Board or Senior Management of your organisation]** through the production of these documents and their minuted approval.

10.3. All staff, contractors and other relevant parties will, therefore, ensure that these are observed in order that we may contribute to the achievement of **[insert organisation name]**'s objectives and the delivery of effective healthcare to the service users.

10.4. These procedures have been approved by the undersigned and will be reviewed on an annual basis.

Name	
Date approved	
Review date	

[02] Staff Handbook – Exemplar Texts

[The following represent exemplar which you may like to insert in the relevant places in your staff handbook.]

[02.1] - Confidentiality & Information Governance (CONTRACTUAL)

During or after your employment at **[insert organisation name here]** (hereafter referred to as "us", "we", or "our"), you must not disclose:

i. any trade secrets *e.g.* financial & staff information or;

ii. other sensitive personal information or confidential information *e.g.* service user medical records & payroll details.

Except where this is necessary for your job or if you are required to do so by law.

You must not remove any documents or items which belong to us or which contain any confidential information from our premises at any time without proper advance authorisation. For example, laptops containing care planning software or staff files.

You must return upon request, and, in any event, upon the termination of your employment, all documents and items which belong to us or which contain or refer to any confidential information and which are in your possession or under your control.

You must, if asked to do so, delete all confidential information from any re-usable material and destroy all other documents and tangible items which contain or refer to any confidential information and which are in your possession or under your control.

In order to provide assurance that access to confidential information is gained only by those individuals that have a legitimate right of access, we undertake monitoring on a regular basis.

Confidentiality audits are also carried out with a view to discover whether confidentiality has been breached.

We have a registered Caldicott Guardian/Information Governance (IG) Lead **[delete as appropriate]** and any requests for sharing of personal information must be authorised.

[Staff must be given access to the policies relating to IG which are set out in the Information Governance Overarching Policy document and this should be evidenced in the employee handbook. Staff must also be made aware of the organisation's procedures and processes around access to confidential information.]

[02.2] – NHS Smartcard Procedures

[Note that this is only applicable for organisations with Smartcards]

If you suspect or witness any breach of NHS Smartcard usage, you should report this to your line manager by using the Information Security Incident Reporting Form.

Your line manager will report all Smartcard related security incidents and breaches to the registered Caldicott Guardian/IG Lead **[delete as appropriate]**.

[02.3] - Physical Security Breaches

If you are concerned that a security breach has occurred or have seen a security breach inform **[insert responsible person here]** and the most senior member of staff on duty immediately of the incident or concern and complete an Information Security Incident Report Form.

If it is believed a crime has been committed, someone has been injured, or an intruder is on site immediately contact the emergency service as appropriate via 999.

If you have identified a potential for a security breach to occur inform your line manager and your organisation's Caldicott Guardian/IG Lead **[Delete as appropriate]** at the earliest opportunity.

[02.4] -Information Security Breaches

Information security breaches are any event or occurrence that has resulted, or could have resulted, in either the disclosure of confidential information to an unauthorised person, put at risk the integrity of the system or data, or put at risk the availability of the system/services and includes all breaches of the Data Protection Act 1998.

If you are concerned that an information security breach has occurred or have witnessed an information security breach inform the Information Governance Lead and the most senior member of staff on duty immediately and complete an incident report form. Information Security Incident Report Forms can be located **[insert location here]**.

[02.5] – Use of Computer Equipment

[Note that this is not applicable if your staff do not have access to computers or digital technology.]

Use of computer equipment, email and the Internet within **[insert organisation name here]** is controlled for security reasons.

[Insert organisation name here]'s policies and procedures which govern digital security can be found **[insert location of policy here.]**

[These policies might include

i. **Not allowing email to be used for personal reasons;**
ii. **The internet only being allowed to be used for business purposes *i.e.* research or e-learning;**
iii. **Password management - see [17] Access Control Procedures for more on this.]**

Auditing and monitoring of employee compliance with the procedures will be ongoing, and failure to comply may result in disciplinary action.

[02.6] – Transfer and Receipt of Personal Information

In the instance that you are required to transfer or receive personal and sensitive information as part of your work duties you must follow the procedures outlined in the Information Handling Procedure Document which can be found at **[insert document location here]**.

Auditing and monitoring of employee compliance with these procedures will be ongoing, and failure to comply with the procedure may result in disciplinary action. If you would like more training on Information Handling, please speak to your line manager.

[02.7] – Record Management

In the course of your work you are required to accurately collect and accurately record service user information. The procedures for carrying out this work are available in our Records Management Policy and Procedure which is located at **[insert location here]**. You will receive training on correct Record Management.

Auditing and monitoring of employee compliance with the procedures will be ongoing, and failure to comply with the procedure may result in disciplinary action. If you would like more training on how to accurately collect and record service user data please speak to your line manager.

[03] Annual IG Audit Checklist (Internal)

Annual Information Governance Audit Checklist (Internal)		
Audit Undertaken by: **[insert IG Lead name]**		
Information Governance Overview (114/Level 3)	**Initial**	**Date**
Annual review of IG Toolkit improvement plan and IG policy. This must be signed off by a senior staff member and dated.		
Routine Staff Monitoring & Compliance Spot Checks (115/Level 3)		
Confirmed that staff members know where to find the IG Policy and understand the policy.		
Contracts (116/Level 3)		
Perform contract spot checks for staff to ensure that there are clauses which identify duty of confidentiality and IG requirements.		
Perform contract spot checks to ensure all agency staff have signed that they have read and understood the Confidentiality Code of Conduct.		
Perform contract spot checks for third party contracts.		
Annual review of contracts to ensure that they reflect any legal requirement changes.		
Staff Training Compliance (117/Level 3)		
Perform staff spot checks to ensure that they understand their Information Governance responsibilities.		
Ensure that all agency staff training records are up to date and that this is evidenced on file.		
Annual review that staff Information Governance training is up to date and effective.		
Service User Consent (202/Level 3)		
Perform regular spot checks to ensure that every service user has a general consent on admission form contained within their care plan.		
Annual review that policy governing service user consent to the use and sharing of confidential personal information is up to date with latest legal guidelines.		
International Data Transfers (209/Level 2b & 3)		
Annual review of information flows to overseas locations.		
Annual review that policy governing International Data Transfers is up to date in terms of new regulations and legislation.		
Service User Information about Sharing of Confidential Data (213/Level 2 & 3)		
Ensure that staff have received & understood training about service user access to their own personal data and care plans.		
Ensure staff are aware of service user complaint procedures.		
Annual review of communications to service users regarding information sharing *e.g.* information leaflet and service user handbook.		
Staff Understanding of Confidentiality Code of Conduct (214/Level 3)		
Confirmed that staff members know where to find the Confidentiality Code of		

Conduct and the purpose of the Code.		
Confirmed that staff members know who the Information Governance Lead is and who to contact for support on Information Governance issues.		
Confirmed that staff know not to look at information about any service user, including any information relating to their family, friends and acquaintances, unless they have a legal reason to do so.		
Confirmed that staff members know that service user information should not normally be shared without service user consent.		
Confirmed that staff working off-site or at home know not to remove personal identifiable information from the premises.		
Annual review of Confidentiality Code of Conduct to keep in line with any new regulations.		
Information Security Processes, Services and Systems (215/Level 3)		
Staff spot checks that they understand the procedures in place and any changes which have been made.		
Annual review that information security processes, services and systems are in line with any new regulations.		
Confidentiality Audit Procedures (216/Level 3)		
Review of Information Security Incident Report forms to see if procedures are adequate.		
Make changes to procedures or guidance to staff if improvements are required.		
Annual review that incident reporting is in line with any new regulations.		
Compliance with NHS Smartcards (304/Level 2 & 3)		
Audit that all NHS Smartcard users have signed the electronic terms and conditions.		
Assess staff understanding and compliance with NHS Smartcard terms and conditions.		
Staff compliance and understanding spot checks have been carried out.		
Information Asset Register (316/Level 3)		
Ensure that Information Asset Register is maintained and updated.		
Security Measures (317/Level 3)		
Confirmed that staff know the correct procedure in the event of unauthorised access to information.		
Annual review of risk assessments to include checks that security measures are working effectively and that they have been updated to reflect any changes to the site or organisation or any new legislation.		
Compliance with Mobile Computing Guidelines (318/Level 3)		
Complete staff spot checks to ensure that they understand mobile computing guidelines and procedures.		
Audit the mobile computing asset register to ensure it is up to date and allocated appropriately.		
Review security, access controls and staff guidance to take into account any changes made to the systems or any new legislation.		

Business Continuity Planning (319/Level 3)		
Review of Business Continuity Plan – must take place regularly		
Incident Management & Reporting Procedure (320/Level 3)		
Confirmed that staff members know who to report information security breaches to.		
Confirmed staff know where the procedures can be located for managing different types of incidents.		
Review security, access controls and staff guidance to take into account any changes made to the systems.		
Access Control (321/Level 3)		
Confirm that access for all users is up to date and monitored and that access rights are at appropriate levels for all staff. Ensure that access rights are revoked for any staff who have left the organisation or for whom access is no longer appropriate. Audit that access control procedures are being followed.		
Allocation of administrator rights is restricted with additional users only granted such rights on authorisation by a senior member of staff.		
Confirm that staff do not share their access rights or otherwise use the system in a way which is counter to that outlined in organisational procedures.		
All staff log out of the computer system.		
Annual review of procedures to ensure system is in line with any new regulations.		
Compliance with Information Flow Procedures (322/Level 3)		
Audit of information flows, methods, locations and data.		
Staff compliance spot checks.		
Annual review of information handling procedures and guidelines to ensure system is in line with any new regulations.		
ICT Network Security (325/Level 3)		
Annual report and review of software system security audits – this may be done by your ICT contractor if this service is offered.		
Staff compliance spot checks.		
Annual review of network security procedures and risk assessments to ensure system is in line with any new regulations.		
Accuracy of service user Information (412/Level 3)		
Annual report and review of care plan audits.		
Staff compliance spot checks.		
Annual review of care plan policies to ensure system is in line with any new regulations.		

Notes:

[04] Staff Contracts – Exemplar Text

[Within your staff contract you must have the following or similar:]

Confidential Information.

You must not disclose any trade secrets or other information of a confidential or sensitive nature relating to **[insert organisation name here]** or any of our associated companies or business or service users and Employees in respect of which we owe an obligation of confidence to any third party during or after your employment except in the proper course of your employment or as required by law.

You must adhere to the Company Information Governance Policy, which is also referred to within the Employee Handbook, it can be found **[insert location here]**. Failure to adhere to this policy may result in disciplinary action.

Full details are contained within the Confidentiality Policy & Procedure **[insert policy number here]** and is also contained in the Employee Handbook.

[05] Third Party Contract – Confidentiality Agreement – Template

Third Party Confidentiality Contract

1. The Parties

1.1. **[Insert organisation name and address here]** referred to in this agreement as "the Company", "we", "us" or "our", and;

1.2. **[Insert name and address of employee/sub-contractor]**, referred to in this agreement as "you" or "your", etc.

2. Purpose of Agreement

2.1. The purpose of this agreement is to provide protection and assurance to both parties that all information, including specifics *i.e.* customer data and information, service user data and information, personal information in relation to clients, service users or colleagues, financial information that is not available to the public (hereinafter referred to as "information"), which has not been made available to the general public by either party and which is either entrusted to or indirectly seen or heard by the other party for whatever reason, will remain confidential, is processed appropriately and protected from inappropriate disclosure. It is of paramount importance that the confidentiality of all service users is protected at all times. You must not disclose or discuss the identity of any service users to anyone outside of the Company, to another consultant, worker or employee while attending another client or disclose any paperwork to anyone outside of the Company, including other service users.

2.2. This agreement shall be binding on assignees, transferees and successors in interest.

3. <u>Agreement</u>

3.1. In consideration of present and future business relationship, and intending to be legally bound, you agree that you will treat as confidential all such information received directly or indirectly from the Company, and will not disclose such information in any way. Where it is necessary to forward any information to an employee or colleague, this access must be limited to that required in order to perform the services requested by the Company.

3.2. Where applicable, you may also have an obligation to comply with the standards for confidentiality and record keeping as set by your professional body.

3.3. All information and specifics *i.e.* related policies, processes and other documentation such as client fees, records, reports, plans, proposals and other papers and items, received or made available by either party shall remain the property of the issuing party and shall be returned upon request. Receipts for all such information shall be signed before delivery.

3.4. You shall provide copies of your policies, procedures or controls to demonstrate that Information Governance requirements have been met, or an acceptable industry standard (*e.g.* ISO 27001 or IASME certificate). Alternatively, you may sign to confirm you adopt our Information Governance policies and procedures.

3.5. The obligation of secrecy and/or otherwise unauthorised use of such information will not be applicable to:

i. Information in the public domain at the time of disclosure as evidenced by printed publications or which becomes a part of the public domain by a publication or otherwise through no fault of the party to whom the information was disclosed.

ii. Information which the receiver can demonstrate was in its possession at the time of the disclosure.

3.6. In submitting information to each other for review, both parties agree that the other party will be under no obligation equitable or contractual, express or implied, except as specified herein.

3.7. The agreement may not be assigned or transferred in whole or part, either voluntarily or by operation of law, by either party, without the express written permission of the other party.

3.8. In the event of a breach of this agreement, you must report the incident immediately or no later than 24 hours after the incident, to the Registered Manager **[insert name and contact details here]**.

3.9. You agree that you will indemnify your services against all losses, claims, costs and expenses arising in connection with any breach of this agreement and will reimburse the Company for any costs or penalties incurred as a direct result of the breach.

4. Termination of Agreement

4.1. This agreement shall remain in effect for the duration of the business relationship between both parties and will terminate seven (7) years after such business relationship has ended.

4.2. This agreement shall be governed by and interpreted through the laws of England and Wales.

5. Declaration

IN WITNESS WHEREOF, the parties hereof have caused this agreement to be duly executed in their names by duly authorised officers.

Signed: [insert employee name] Date:

For and on behalf of: [insert company name]

Signed: [insert third party name] Date:

For and on behalf of: [insert third party company name]

[06] Confidentiality Policy (including monitoring & auditing access) – Exemplar Texts

[06.1] Policy Description

[This text, or similar, should be inserted into your policy description]

Confidential Information should be shared in line with the 7 Caldicott Principles 2016: http://informationsharing.org.uk/wp-content/uploads/2016/05/Caldicott-principles.pdf.

The purpose of this policy is to outline the principles which must be observed by the employees of **[insert organisation here]** who have access to any personal, sensitive personal or otherwise confidential information. This policy protects and safeguards sensitive personal information and confidential information as is required by law (including, but not limited to, the Data Protection Act 1998, Health & Social Care Act 2012, and the Common Law duty of confidentiality).

Information can relate to service users and employees (inclusive of Agency or temporary employees) however stored. Information may be held on paper, stored digitally (*e.g.* on CD/DVD, laptop, computer file etc.) or heard by word of mouth.

[06.2] Outline of Procedures

[This text, or similar, should be included in your procedure outline]

Storage of personnel documents, including the archiving room, needs to be kept under lock and key at all times.

Staff must retain personal and confidential information and data securely in locked storage when not in use, and keys should not be left in the barrels of filing cabinets and doors.

All nurse stations and administrative offices **[insert any other location where confidential information is stored]**, when left unoccupied, must be locked unless all personal and confidential information has first been cleared off work stations/desks and secured in locked storage.

Access to electronic data should be limited to essential users only. Computer users must ensure their screens are locked prior to leaving their desktop/laptop, including all computing devices used for care planning. These procedures are outlined in the Access Control procedures which are located **[insert location here]**.

Photographs and video or sound recordings should not be shared without the express consent of service users, staff members or their legal advocates.

No mobile phones, tablets, recording devices or cameras are to be kept within the service user's environment. All devices should be locked away in the storage areas provided. **[Note that if your organisation uses mobile devices as part of your service then this would not be applicable, though a separate risk assessment should be completed for this.]**

[06.3] Disclosure

[This text, or similar, should be included in your disclosure]

[Insert organisation name here] has a registered Caldicott Guardian/Information Governance (IG) Lead **[delete as appropriate]** and any requests for sharing of personal information must be authorized by this individual.

[06.4] Policy – Monitoring and Auditing Access

[This text, or similar, should be inserted into your policy]

1. <u>Monitoring Access to Confidential Information</u>

1.1. In order to provide assurance that access to confidential information is gained only by those individuals that have a legitimate right of access, it is necessary for appropriate monitoring to be undertaken on a regular basis. Compliance monitoring will be carried out by **[Insert responsible individual's name and position here]** in order that irregularities regarding access to confidential information can be identified, reported to the IG Lead and action taken to address the situation, either through disciplinary action, the implementation of additional controls or other remedial action as necessary.

1.2. Actual or potential breaches of confidentiality should be reported to the registered Caldicott Guardian/IG Lead **[delete as appropriate]** immediately on the appropriate incident reporting form, in order that action can be taken to prevent further breaches taking place.

1.3. Should unauthorised access to confidential information be gained by any individual, this will be dealt with in accordance with disciplinary procedures.

1.4. In the instance of a data security breach, the procedures outlined in the Data Security Breach policy & procedure will be followed.

2. <u>Auditing Access to Confidential Information</u>

2.1. Confidentiality audits will focus on controls within electronic records management systems and paper record systems; the purpose being to discover whether confidentiality has been breached, or put at risk through deliberate misuse of systems, or as a result of insufficient controls. Audits of security and access arrangements within each area are to be conducted on a six-monthly rolling programme. **[How frequently you audit information can vary, but as a minimum there should be a full annual audit]**

2.2. [Audits should include some or all of the following as deemed appropriate by the registered Caldicott Guardian/IG Lead]:

i. Failed attempts to access confidential information;

ii. Repeated attempts to access confidential information;

iii. Access of confidential information by unauthorised persons;

iv. Previous confidentiality incidents and actions, including disciplinary, taken;

v. Staff awareness of policies and guidelines concerning confidentiality and understanding of their responsibilities with regard to confidentiality;

vi. Appropriate communications with service users;

vii. Verbal conversations with personal data exchange;

viii. Appropriate recording and/or use of consent forms;

ix. Appropriate allocation of access rights to confidential information;

x. Appropriate staff access to physical areas;

xi. Storage of and access to filed hard copy service user notes and information;

xii. Correct process used to securely transfer personal information by post or fax;

xiii. Appropriate use and security of desk and mobile devices in open areas;

xiv. Confidential information sent or received via e-mail, security applied and e-mail system used;

xv. Security applied to PCs, laptops and mobile electronic devices;

xvi. Evidence of secure waste disposal;

xvii. Use of whiteboards or similar for confidential information;

xviii. Information flows of confidential information;

xix. Appropriate transfer and sharing arrangements are in place;

xx. Security and arrangements for recording access applied to manual files both live and archive, *e.g.* storage in locked cabinets/locked rooms.

xxi. Appropriate staff use of computer systems, *e.g.* no excessive personal use, no attempting to download software without authorisation, use of social media, attempted connection of unauthorised devices etc.

3. Audit Method

3.1. Audits will be carried out as required by some or all of these methods:

i. Unannounced spot checks to random work areas;

ii. A series of interviews with management and staff, where a department or area of the organisation have been identified for a confidentiality audit. These audits will be carried out by the registered Caldicott Guardian/IG Lead **[delete as appropriate]** or their Deputy;

iii. Based on electronic reports [This can be from your ICT contractor or from internal monitoring. Note that this can be deleted if you do not store or share information digitally.]

iv. Based on electronic reports from care planning software or auditing of care plans. [This can be from your ICT contractor or from internal monitoring. Note that this can be deleted if you do not store or share information digitally.]

4. <u>Breach of Confidentiality</u>

4.1. All staff should be aware that access, processing or transfer of personal sensitive information is monitored and audited. Any breach of security or infringement of confidentiality through either verbal, hard copy or electronic media may be regarded as serious misconduct, which would lead to disciplinary action or dismissal in accordance with disciplinary procedures. In addition, unauthorised disclosure of personal information is an offence and could lead to prosecution of individuals and/or the organisation.

[07] Information Asset Register – Template

[**The table below contain examples of the types of information which would be recorded in an information asset register. You can add/delete rows as necessary.**

Only complete cells 5a-d if you answer "Yes" in column 5: "Does it store confidential and sensitive personal information?" These columns are marked in yellow.

Column 5c: European Economic Area countries are countries in the EU plus Iceland, Liechtenstein and Norway:

- Austria
- Belgium
- Bulgaria
- Croatia
- Cyprus
- Czech Republic
- Denmark
- Estonia
- Finland
- France
- Germany
- Greece
- Hungary
- Iceland
- Ireland
- Italy
- Latvia
- Liechtenstein
- Lithuania
- Luxembourg
- Malta
- Netherlands
- Norway
- Poland
- Portugal
- Romania
- Slovakia
- Slovenia
- Spain
- Sweden
- United Kingdom

Transferring sensitive and confidential information outside of these countries is tightly regulated. Advice can be found here: https://ico.org.uk/for-organisations/guide-to-data-protection/principle-8-international/**. If in doubt, contact the ICO for further advice and guidance.]**

1	2	3	4	5	5a	5b	5c	5d	6	7	8	9	10	11
Asset Type	**Make and Model**	**Serial Number**	**What is stored?**	**Does it store confidential or sensitive personal information?**	**What is it used for?**	**Who is it shared with?**	**Is it shared outside of the EEA?**	**What is the legal basis for using or sharing it?**	**Software Installed**	**Responsible Owner**	**Security Measures**	**Support Contact**	**Asset Issued**	**Asset Returned**
e.g. Desktop Computer, paper care records, staff files, laptop, smart phone	e.g. HP Pavilion, Paper records in cabinet	e.g. HP123456, Laptop 1, Filing cabinet 1	e.g. Patient records, payroll, staff contact details	Yes or No [Note that confidential and sensitive personal information are legal terms]	e.g. care planning	e.g. GP	Yes or No	e.g. Health & Social Care Act 2012, Employment Act 2008	e.g. Microsoft Office package; Windows 10; service user admin system	e.g. IG Lead, staff member with portable device, Nurse Manager	e.g. Password protected, locked in archive cage	e.g. Mark at IT Direct - 01234 567891	01/01/01	01/02/02

[08] General Consent on Admission Form – Exemplar Text

[Insert the following text, or similar, into your General Consent on Admission form]

I, **[insert service user name here]**, have received and understood the leaflet detailing my right to confidentiality as outlined by law, including but not limited to the Data Protection Act 1998, Health & Social Care Act 2012, and the Common Law Duty of Confidentiality.

I, **[insert service user name here]**, understand that if I have any concerns regarding the use or sharing of my personal confidential information I can raise those concerns by **[insert your organisation's process here – this should also be outlined in your service user handbook.]**

[As ever, it is important that the service user has given informed consent to the use and sharing of their personal information for the purpose of their care.]

[09] Service User Handbook – Exemplar Text

[09.1] Use of Confidential Personal Information

[Insert the following text, or similar, into your service user handbook]

Personal information about you will be stored in paper form and on the computer **[Delete if not relevant]**. Both methods of data storage are kept strictly confidential. **[You may wish to refer to your Record Keeping policy here]**.

In the interest of providing you with high quality care, some personal information will be shared with your care team. In the instance that your personal information is required by external professionals or visitors **[insert your organisation's procedure for sharing of confidential personal information with third parties here, this should be detailed in your Information Handling policy or similar]**.

In addition to personal care, some of your confidential information may need to be shared for the following reasons: **[insert additional reasons here *i.e.* for improvements to your organisation in line with service user needs]**.

If you are receiving support or care from other organisations, your personal information may need to be shared with them. This is always done in line with legislation, such as the Data Protection Act 1998, which regulates the safe sharing of personal data. The external organisations who may require your information include:

i. GPs

ii. District Nurses

iii. Other health professionals
iv. Social Workers
v. Care Quality Commission

Every person has the right to access their own personal information. **[insert your service user access to information procedures here]**.

We commit to the following in order to ensure that your information is shared appropriately and kept confidential: **[delete or add as appropriate]**

i. Staff will not discuss you or your affairs within earshot of anyone not directly concerned with your care.
ii. Discussion of you and your affairs will be for the purposes of managing and improving care, and not as entertainment or gossip.
iii. You will always be offered privacy for personal discussions.
iv. Records will be designed, used and stored so as to assure privacy. Legislative controls over records, such as the Data Protection Act 1998 and Information Governance, will be adhered to, and your explicit permission in writing will be sought before information is passed to any person other than those directly concerned with your care.
v. Access to information – You have the right to information about the objectives of your care and a detailed explanation of the service being offered and how your information is used and shared for the purposes of ongoing care
vi. **[Insert organisation name here]** ensures that access to the premises is controlled at all times.

vii. All visitors must sign our Visitors' Book, so that staff are aware of who is on the premises.

viii. For the safety of you and our staff there is CCTV in all public areas within the organisation and externally.

[09.2] Confidentiality Clause

[The following text, or similar, needs to be inserted within your confidentiality clause. Note that your policies, procedures and systems may have different names. This must be updated to reflect the nomenclature within your organisation.]

[Insert IG Lead name here] is a registered Caldicott Guardian/Information Governance Lead **[delete as appropriate]**, who is responsible for protecting the confidentiality of all service users' information and enabling appropriate information sharing.

It is of paramount importance to ensure that confidential information about service users is efficiently managed, and in that regard, our Information Governance policy, Staff Confidentiality Code of Conduct and management accountability and structures provide a robust governance framework for information management.

[10] Service User Leaflet

The following leaflet is aimed at service users and should be adapted for your organisation specifically.

How we keep your personal information safe:

We have a duty to:

- Maintain full and accurate records of the care we provide;
- Keep records about you confidential, secure and accurate;
- Provide information in a format that is accessible to you (*i.e.*, in large type if you are partially sighted).

We **will not** share information that identifies you for any reason, unless:

- you ask us to do so;
- we ask and you give us specific permission;
- we have to do this by law;
- we have special permission for health or research purposes

We may share your information, with your consent and always in line with our information sharing procedures, with:

1. Social Services
2. Hospital Services
3. Local Authorities
4. Your GP
5. Your family or representative

Anyone who receives information from us also has a legal duty to keep it confidential.

If you require this leaflet in a different format or you need further information or assistance, please contact:

[insert your organisation's contact details here]

Keeping Your Information Safe!

This leaflet explains:

- **How we keep your personal information confidential**
- **Who we share information with**
- **How we use your information**
- **How you can access your records**

Why we collect information about you:

We aim to provide you with the highest quality of care. To do this we must have access to your medical records and keep care plans to monitor and improve your daily care.

These records may include:

- Basic details about you, such as address, date of birth, next of kin
- Contact we have had with you such as clinical visits
- Notes and reports about your health
- Details and records about your treatment and care
- Relevant information from people who care for you and know you well, such as care professionals and relatives

It is our promise to you that we will:

- discuss and agree what we record about you
- give you access to your records whether digital or paper based
- keep you informed about, and ensure that, you have input into your care plan

Your records with us may be stored on paper or on the computer – if you would like to know what measures we have to keep your records safe, please ask!

How we use your records:

The people who care for you use your records to:

- Provide a good basis for all health decisions made by you and care professionals
- Allow you to work with those providing care
- Make sure your care is safe and effective, and
- Work effectively with others providing you with care

Others may also need to use records about you to:

- Check the quality of care (such as clinical audit)
- Protect the health of the general public
- Manage social care services
- Help investigate any concerns or complaints you or your family have about your care

We always seek your consent before sharing any aspect of your personal information. If you are not able to provide consent, your representative with an appropriate power of attorney or the clinical team can make a decision in your best interests.

Your rights:

You have the right to confidentiality under the Data Protection Act 1998 (DPA), the Human Rights Act 1998 and the common-law duty of confidentiality (the Disability Discrimination and the Race Relations Acts may also apply).

You have the right to ask for a copy of all records about you. Please speak to a member of staff to see your records. If you think anything is inaccurate or incorrect, please let us know.

Notification:

Social Care information sharing is subject to the principles which have been set out by the National Data guardian in the Caldicott Reports of 2013 and 2016.

The Data Protection Act 1998 requires organisations to notify the Information Commissioner's Office (ICO) of the purposes for which they process personal information: www.ico.org.uk

If you have any concerns or questions about the use of your personal information please let us know.

[11] Information Security Incident Report Form – Template

Information Security Incident Report Form			
Date incident reported:		Date incident occurred:	
Location of Incident:			
What is being reported:	□Near-miss □Information security breach. *If this option is selected, speak to IG Lead* immediately to report the breach with the IG Toolkit Incident Reporting Tool.		
Type of information Indicate what form the information was in when the incident occurred	□Digital □Verbal □Paper □Smartcard		
Details of Incident: (State facts only and **not** opinions. Include details of staff involved and any contributing factors)			
Action to be taken:			

Outcome of action:			
Lessons Learnt:			
Has the IG Lead been informed?	Yes □ No □	Has the IG Toolkit Incident Reporting Form been completed?	Yes □ No □
Reporter details			
Name:		Job title:	
Information Governance Lead follow up	(investigations, findings and planned actions)		
IG Lead Name:		Date:	

[12] Assignment of Mobile Computing Equipment Form – Template

ASSET CONTROL FORM		
Type of asset [tick]:		Make and model:
Laptop Mobile phone Memory stick External hard drive PDA Other [insert type] …………………………….		
If the asset is a mobile phone, enter number:		Serial number:
Date entered on asset register:	Equipment is Encrypted: [circle] YES NO N/A	Indelibly marked to indicate the property of the organisation: [circle] YES NO
STAFF INFORMATION		
Allocated to: Job role:		

STAFF DECLARATION

I, [print name] ………………………………………………………. understand and agree to comply with the staff guidelines on using mobile computing devices and related procedures covering good Information Governance.

I understand that:

- It is my responsibility to report **immediately** any theft, loss, damage or misuse of the above asset using the Information Security Incident Report Form.
- The equipment must be returned if I leave the employ of the organisation and that a final salary deduction may be made if equipment is not returned.
- Failure to comply with the above could lead to disciplinary action or incur financial penalties.

Signed: Dated:

[13] Staff Guidelines: Using Mobile Computing Equipment - Template

[It is important that you consider whether or not you will allow staff to use their personal equipment in relation to their work. Allowing the use of personal devices has a long list of benefits in terms of lower costs and increasing efficiency, but also increases risks which you must mitigate and assess. The following guidelines assume that authorised personnel can use mobile computing devices which have been issued by the organisation so will need to be amended if personal devices are being used.

These guidelines are not applicable if no mobile computing devices are used in your organisation; however, you should state in one of your policies that no mobile computing devices are used.]

1. Introduction

1.1. These guidelines govern the use of portable computer devices and removable media, collectively known as mobile computing equipment. These guidelines recognise the increased risk to personal information incurred through the use of mobile computing devices and they complement, but do not replace, our procedures and guidelines regarding protecting service user information. **[you may wish to name policies here *i.e.* Records Management policy etc.]**

2. Purpose

2.1. These guidelines aim to support staff members in **[insert organisation name]** (hereafter referred to as "us", "we", or "our") who are authorised to use mobile computing equipment by ensuring they are aware of the risks of mobile computing and comply with confidentiality and security issues.

3. Scope

3.1. The guidelines cover the mobile computing equipment set out below when it has been purchased or authorised by us. It does not include any equipment owned by staff or those brought into the organisation from a previous organisation. The guidelines apply to all staff including permanent, temporary, and agency.

i. *Portable computer devices* - includes laptops, notebooks, tablet computers, and Smartphones *e.g.* iPhones etc.;

ii. *Removable data storage media* - includes any physical item that can be used to store and/or move information and requires another device to access it. For example, CD, DVD, tape, digital storage device (flash memory cards, USB memory sticks, portable hard drives). Essentially anything that data can be copied, saved or written to which can then be taken away and restored on another computer.

4. Authorisation

4.1. Only authorised staff should have access to mobile computing equipment. Any member of staff allowing access to any unauthorised person deliberately or inadvertently may be subject to disciplinary action.

4.2. Staff should **not** use their own (or unauthorised) computing equipment for our business. **[note that this might not be true in your organisation]**

5. <u>Be aware of security measures in place</u>

5.1. To reduce the risk of loss and unauthorised access we have put the following measures in place: [note that this section should be updated with your organisation's procedures, which might include the following:]

i. An asset control form is completed for each mobile computing device provided to a staff member; and this person is listed in the Information Asset Register as the nominated responsible owner;

ii. All equipment is security marked with a UV pen;

iii. Encryption **[name encryption type here *e.g.* VeraCrypt etc.]** is applied to all mobile computing equipment;

iv. Password protected screensavers are installed on laptops;

v. Anti-virus software **[name type]** is in use and is regularly updated **[insert how often]**;

vi. Regular backups are taken of the data stored on the mobile equipment;

vii. Disposal and re-issue of mobile computing equipment is recorded in the Information Asset Register.

6. <u>Recognise the risks and comply with your responsibilities</u>

[Again, ensure that the following echo your own procedures]

6.1. You should ensure you DO:

i. Store mobile equipment securely when not in use on and off site;

ii. Ensure files containing personal or confidential data are adequately protected *e.g.* encrypted and password protected;

iii. Virus check all removable media *e.g.* memory sticks etc. prior to use;

iv. Obtain authorisation before you remove mobile equipment from the premises;

v. Be aware that software and any data files created by you on our mobile computer equipment are our property;

vi. Report **immediately** any stolen mobile equipment to the police and your line manager (failure to report a stolen mobile phone could result in significant charges from our telecoms provider). An incident report form must be completed;

vii. Be aware that the security of your mobile computer equipment is **your** responsibility;

viii. Ensure that mobile equipment is returned to us if you are leaving employment (A final salary deduction may be made if equipment is not returned).

6.2. You should ensure you DO NOT:

i. Disable the virus protection software or bypass any other security measures put in place by us;

ii. Store personal information on mobile equipment unless the equipment is protected with encryption, and it is absolutely necessary to do so;

iii. Remove personal information off site without authorisation;

iv. Use mobile computer equipment outside of our premises without authorisation;

v. Use your own mobile computer equipment for the organisation's business;

vi. Allow unauthorised personnel/friends/relatives to use mobile equipment in your charge;

vii. Leave mobile equipment in places where anyone can easily steal them;

viii. Leave mobile equipment visible in the car when traveling between locations;

ix. Leave mobile equipment in an unattended car;

x. Leave mobile equipment unattended in a public place *e.g.* hotel rooms, train luggage racks;

xi. Install unauthorised software or download software / data from the Internet;

xii. Delay in reporting lost or stolen equipment.

7. Approval

7.1. These procedures have been approved by the undersigned and will be reviewed on an annual basis.

Name	
Date approved	
Review date	

[14] Business Impact Analysis Document - Template

Risk Assessment Descriptors: Use the descriptors below to assess the LIKELIHOOD of a risk occurring					
Score	5	4	3	2	1
Descriptor	Probable	Possible	Unlikely	Rare	Negligible
Likelihood of occurrence	More likely to occur than not	Reasonable chance of occurring	Unlikely to occur	Will only occur in rare circumstances	Will only occur in exceptional circumstances
	greater than 50% chance	between 50% and 5%	between 5% and 0.5%	between 0.5% and 0.05%	between 0.05% and 0.005%
	greater than 1 in 2 chance	1 in 20 chance	1 in 200 chance	1 in 2000 chance	1 in 20,000 chance
Risk Impact: Use the descriptors below to assess the IMPACT severity if a risk occurs					
Score	5	4	3	2	1
Descriptor	Catastrophic	Major	Moderate	Minor	Insignificant
Severity of impact	Permanent loss of core service or facility	Sustained loss of service which has serious impact on delivery of care.	Some disruption in service & unacceptable impact on care. Non-permanent loss of ability to provide a service	Short term disruption to service with minor impact on care	Interruption in a service which does not impact on the delivery of care or the ability to continue to provide a service

Record the likelihood and impact of potential hazards and/or threats together with the recovery time-frame options.					
			Option 1	Option 2	Option 3
Hazard or threat	Likelihood Score	Impact Score	(2 hours)	(24 hours or more)	(5 days or more)
Loss of main premises					
Loss of computer systems/ essential data					
Loss of telephone system					
Loss of essential supplies					
Loss of health records					
Incapacity of lead professional					
Incapacity of support staff					
Loss of electricity supply					
Loss of gas supply/ heating					
Loss of water supply					
Loss of security systems					

[15] Emergency & Business Continuity Plan – Exemplar Text

[The following text, or similar, should be inserted into your Business Continuity Plan. It details procedures relating to Information Governance. Please note that this plan assumes that you are using paperless working as far as possible and that you might have digital care planning software, if this is not the case then not all of the following would need to be included in your plan. Your IT supplier or support will be able to help with this.]

Business Continuity Plan

In the instance that there is a loss of the main premises, **[insert name here]** will need to contact the ICT supplier regarding data restoration. The ICT supplier is **[insert supplier name here]** and they can be contacted **[insert contact details here]**.

1. Information Assets

1.1. **[Insert organisation name here]** maintains, separately to this document, an Information Asset Register which contains details of all information assets pertinent to the business. This register is stored **[insert hard copy location and location on computer system of Information Asset Register].**

2. Loss of computer system/essential data

2.1. The supplier must be notified immediately if either computer hardware or the core software are lost **[insert contact details]**. The equipment and software will ultimately be replaced, but short term, it has been agreed that the following will be made available at **[insert name of temporary accommodation]**:

i. PC’s and printers to enable business continuity;

ii. Access to a photocopier;

iii. Access to a fax machine;

iv. The facility to scan and attach post [this would not be classed as urgent to ensure business continuity in the short term].

2.2. Computer backups are made **[insert how often. If applicable, you may wish to state which files are backed up].** Any information assets selected for backup are encrypted during the backup process using **[insert encryption type here]**. There is no transmission of information assets in an unencrypted form. The key for the encryption is held in the following places: **[insert location]**

2.3. The transmission of the encrypted data files is done using an authenticated and IP address restricted FTP server. All data in transit is encrypted prior to transmission and all data at rest is stored in an encrypted format. **[Insert how long you retain backups for here. This sounds complicated, but your ICT supplier or support should be able to help and provide advice on what would be appropriate for your organisation.]**

2.4. The Information Asset Register contains information on mobile devices with secure remote access to the care planning system. These may be available to facilitate immediate access if the server is unaffected. **[if your organisation does not use digital care planning software then this will not be relevant for you.]**

3. Recording data

3.1. If there is a failure in the ICT system or any standalone computer, the staff will revert to a paper backup system to capture that important data so this can be recorded on the system retrospectively. Templates for recording information when the system is unavailable can be found **[insert location]**.

3.2. Once information is captured on the paper templates these are kept securely **[insert location here]** until they can be entered onto the computer system. Once they have been entered and validated the paper documents are securely disposed of. **[If you do not run a paperless system, then your usual storage procedures should be followed. If you do not revert to a paper system in case of a failure in the ICT system, then detail your procedures here instead.]**

4. Loss of care records

4.1. Paper care records are stored in cabinets in **[insert location]**, and are protected from any untoward event by **[insert your organisation's procedures here]**.

4.2. **[insert number]**% are summarised onto the care planning system and could be reconstructed from data held on the computer system if necessary.

[16] Data Security Breach Procedures – Exemplar Text

[insert the following, or similar, into your Data Security Breach Procedure]

Where it is suspected that a data security breach or Information Governance Serious Incident Requiring Investigation (SIRI) has taken place, it is good practice to informally notify key staff (Responsible person, IG Lead etc.) as an 'early warning' to ensure that they are in a position to respond to enquiries from third parties and to avoid 'surprises'. For cyber incidents notify **[insert name & position of person responsible for ICT here]**.

From 1st June 2013, all organisations processing Health and Social Care personal data are required to use the NHS IG Toolkit Incident Reporting Tool to report level 2 IG SIRIs to the Department of Health (DH), Information Commissioner's Office (ICO) and other regulators. Level 2 IG SIRIs are sufficiently high-profile cases or deemed a breach of the Data Protection Act 1998 or Common Law Duty of Confidentiality, and hence reportable to the DH and ICO.

In the case of an information security incident:

i. An Information Security Incident Report Form should be completed and given to the registered Caldicott Guardian/IG Lead **[delete as appropriate]**.
ii. If the breach is a Level 2 serious incident it must be reported on the IG Toolkit Incident Reporting Tool within 24 hours with as much information as is available at the time.

iii. **[Insert organisation name here]** will continue to investigate the incident and upload a full report to the IG Toolkit Reporting Tool within 5 days of the initial report having been made.

iv. The registered Caldicott Guardian/IG Lead **[delete as appropriate]** is responsible for the completion of the reporting tool, for providing details of the incident to **[insert name of appropriate person here]**, and to auditing procedures and processes to prevent reoccurrence.

Where incidents occur out of hours, staff are to contact the Responsible Person and/or the Home Manager **[delete as applicable]** who will take action to inform the appropriate contacts. If the IG Toolkit Reporting Tool is completed with details of a Level Two security breach, the ICO is automatically informed.

[17] Access Control policy & procedures & Access Management Log – Template

[This policy covers both hard copy and digital storage of information, if you do not use one of these then delete as appropriate.]

Access Control Policy & Procedures

1. Introduction

1.1. Information is stored throughout the organisation to facilitate the safeguarding and sharing of information.

2. Purpose

2.1. These Access Control Procedures set out how **[insert organisation name]** (hereafter referred to as "us", "we", or "our") will allocate, manage and remove access rights to systems holding personal sensitive information so that only authorised personnel have access to use and share information held within those systems; and they aim to ensure that access rights are used appropriately by our staff.

3. Scope

3.1. These procedures relate to access controls for information systems used to store confidential data. This can include:

i. Hard copy storage of confidential and sensitive personal information;

ii. Digital storage of confidential and sensitive personal information.

4. Summary of technical access controls

4.1. Hardcopy storage

i. All paper documents (hard copy) which contain sensitive personal or confidential information are recorded on the Information Asset Register (IAR). The documents are locked away unless in a room which is in use. Access to sensitive personal or confidential information is restricted to those who have a legal basis for access.

4.2. Digital storage

i. All digitally stored information which contain sensitive personal or confidential information are recorded on the IAR. The IAR outlines the technical controls which are in place across all computer systems and information storage devices. Technical access controls have been built into our systems by **[insert ICT supplier/support name here (if applicable)]** to ensure that confidential information is protected.

4.3. The IAR is located **[insert IAR location here]**.

5. Responsibility for user access management

5.1. As stated in our Information Governance policy the Caldicott Guardian/IG Lead is responsible for access rights to confidential and sensitive personal information. All access rights will be recorded on the Access Management Log which is located **[insert location here]**.

6. Access Management procedures for Hardcopy Storage

[Your procedures may resemble the following but add or remove as is applicable for your organisation.]

6.1. The IAR shall contain the location of all confidential and sensitive personal information.

6.2. Each storage location will have a risk assessment to ensure that the data is properly secured.

6.3. A record will be kept of who has access to each storage location.

6.4. An audit will be completed at least annually by the IG Lead to ensure that the information is secured properly and that access is restricted to those who have a legal requirement to use the information.

7. Access management procedures for Digital Storage

[insert your own procedures here which may resemble the following:]

7.1. Each user is identified by a unique user ID so that users can be linked to and made responsible for their actions.

7.2. The use of group IDs is only permitted where they are suitable for the work carried out **[insert examples here if applicable]**.

7.3. During their induction to the system, each user is trained on the use of the system, given their user login details, and is required to sign to indicate that they understand the conditions of access.

7.4. A record is kept of all users given access to the system. This record can be found **[insert location here]**.

7.5. In the instance that there are changes to user access requirements

i. Changes to requirements will normally relate to an alteration to the level of access used or suspension of an account, *e.g.* **[insert possible reasons here *i.e.* promotion or long-term leave]**.

ii. Changes to access can only be authorised by **[insert name here]**.

7.6. Password management

[Insert your password management procedure here. These may resemble the following:

i. Strong passwords – three random words create a strong password. Staff can still utilise numbers and special characters.

a. **The random words must not reference the user's name, the name of friends or any family member, place of birth, location, holiday location, pet's name or similarly easy to guess word.**

ii. Users must not share their password with anyone. If users are found to have been sharing passwords this is a breach of [insert organisation name here]'s policies and may cause disciplinary action to be taken.

iii. Passwords must be changed every [insert number here] days.]

7.7. Removal of users

i. As soon as an individual leaves, all their system logons are revoked;

ii. As part of the employee termination process line managers inform **[insert name here]** of all leavers and their date of leaving and they are responsible with the removal of access rights from the computer system;

iii. The IG Lead reviews all access rights on a regular basis, but in any event at least once a year. The review is designed to positively confirm all system users. Any lapsed or unwanted logons, which are identified, are disabled immediately and deleted unless positively reconfirmed.

8. Monitoring compliance with access rights

8.1. The management of access rights is subject to regular compliance checks to ensure that this procedure is being followed and that staff are complying with their duty to use their access rights in an appropriate manner.

8.2. Areas considered in the compliance check include whether:

i. Allocation of administrator rights is restricted;

ii. Access rights are regularly reviewed;

iii. There is any evidence of staff sharing their access rights;

iv. Staff are appropriately logging out of the system.

9. Approval

9.1. These procedures have been approved by the undersigned and will be reviewed on an annual basis.

Name	
Date approved	
Review date	

Access Management Log – Template

User ID	Name	Access Level	Start Date	Access Authorised by:	End Date	Date Access Removed	Access Removed by:
e.g. 157	e.g. Joe Bloggs	e.g. Administrator	e.g. 01/01/2002	e.g. Bill	e.g. 28/05/2016	e.g. 28/05/2016	e.g. Ben
e.g. 158	e.g. Fred Anderson	e.g. ~~user~~ Administrator	e.g. ~~20/02/2015~~ 17/12/2015	e.g. ~~Bill~~ Ben	e.g. 28/05/2016	e.g. 28/05/2016	e.g. Ben

[18] Staff Guidelines on The Appropriate Use of Computer Systems – Template

[These guidelines apply to all staff including permanent, temporary, and agency. These guidelines, or similar, should be included in your staff training materials]

Staff Guidelines

1. Preventing unauthorised system access

1.1. Whenever you leave your desktop computer unattended, get into the habit of locking it so that information cannot be accessed by unauthorised persons. To quickly lock your computer, press Ctrl, Alt and Delete together and then select "lock computer", alternatively you can press the Windows Key +L, this will then require you to input your password before information and applications can be accessed again.

1.2. When leaving your work station for the day, log out of the system entirely and close down the computer.

2. Password management

[Insert your password management procedure here. There are example password management procedures in [17] Access Management Procedures.]

3. Personal use of ICT equipment

[If you do not allow access to Computer equipment at all, then state that here.]

3.1. ICT facilities such as the Internet and email have been provided by **[insert organisation name here]** primarily for business purposes. **[Insert**

organisation name here] does not permit the personal use of these facilities.

3.2. Inappropriate use of the ICT systems is a disciplinary offence and may lead to dismissal.

3.3. Inappropriate use includes but is not limited to: accessing or downloading pornographic or offensive images and material, or sending harassing or offensive emails, **[insert other examples, if appropriate]**.

4. Appropriate use of email

4.1. Do not keep Spam email or forward it to other people; do, however, delete them.

4.2. Do not open emails or attachments from unrecognised or suspicious email accounts.

4.3. Never reply to junk email.

4.4. You are expected to manage your email in a professional manner. Email at work is primarily provided for work purposes. In **[insert organisation name here]**, staff may not use the system for personal mail. **[Delete if not applicable]**

5. Audit trails and reporting security breaches

5.1. Nearly all of the activity you perform on a computer can be tracked. **[Insert your organisation's procedures for auditing computer usage *e.g.* backups, internet monitoring etc. This service can often be provided by your ICT Supplier or Support.]**

5.2. Recorded information will be used to aid an investigation where breaches of security, the law or these guidelines are suspected. This information is kept confidential, but when used helps to explain innocent situations more often than exposing security breaches.

5.3. Information security breaches might involve unauthorised use of equipment or unauthorised access to data. Any breach of security, however small, wastes time and often requires work to be repeated and could be a potential risk to the organisation or individuals.

5.4. If you know or suspect that a breach of information security has occurred, please inform your Information Governance lead **[insert name]** by completing the Information Security Incident Report Form. This includes reporting near-misses.

6. Unlicensed software and computer viruses

6.1. You should never install or use software that hasn't been authorised by **[insert organisation name here]** on your work computer. The main reasons why you should never do this are:

i. The risk of infection to your computer, other computers and the network **[if applicable]** from malicious code embedded in the software. The risk applies to all programs and games downloaded from the Internet, on CD or any other storage media. Malicious code includes computer viruses and spyware, and the effects will vary depending on which has been downloaded. Some malicious code will just waste time while another can destroy data or even allow a malicious user to gain access to your computer;

ii. The likelihood of breaching copyright and licensing laws. [**Insert organisation name here]** has to pay for a license for the software used on its systems. If you install software without authorisation this process is by-passed and you put the organisation at risk of legal action from the owner of the software. If you are installing so-called free software it could be an illegal copy, or it could be trial software with an expiry date. Even if neither of these things apply, the software is likely to be for single personal use and require a license for corporate use;

iii. The download may interfere with our software, causing it to run more slowly or not work at all.

6.2. If you find some software you think **[insert organisation name]** could benefit from, please inform the IG Lead.

6.3. Malicious code (viruses) may also be contained within email attachments. **[Insert organisation name here]** has an anti-virus system that will catch most incoming viruses on emails, but always be cautious of email attachments from people you don't know.

7. Approval

7.1. These guidelines have been approved by the undersigned and will be reviewed on an annual basis.

Name	
Date approved	
Review date	

[19] Information Handling Policy Procedures - Template

Information Handling Policy & Procedures

1. Introduction

1.1. It is important that measures are put in place to protect confidential information from unauthorised access or disclosure, loss, destruction or damage.

1.2. No matter how it is collected, recorded and used (*e.g.* on a computer or on paper) confidential information must be used and transferred in accordance with legal requirements, such as the Data Protection Act 1998 and the Common Law Duty of Confidentiality.

2. Purpose

2.1. Information Handling Procedures ensure that personal information is protected and that it is not disclosed inappropriately, either by accident or design, whilst in use in **[insert organisation name here]** (hereafter referred to as "us", "we", or "our"), or when it is being transferred or communicated to and from the organisation.

3. Scope

3.1. We collect personal information about people with whom it deals in order to carry out its business and provide its services.

3.2. Such people include service users, staff (present, past and prospective), suppliers and other business contacts. The procedure applies to all staff.

4. Secure use of personal information

4.1. Guidelines for staff on the secure use of personal information are outlined in the staff handbook and staff code of confidentiality.

5. Secure receipt and transfer of personal information

We ensure that there are secure points for the receipt of personal information transferred to us and we have applied the following measures to safeguard personal information during receipt and transfer/transit:

5.1. *Verbal communications:*

Staff members have been provided with guidance on verbal communications including:

i. Taking appropriate precautions not to reveal confidential information *e.g.* to avoid being overheard when making a phone call;

ii. Not having confidential conversations in public places or open offices;

5.2. *Postal services and couriers:*

To ensure that confidential information transferred from the organisation by post or courier is done so as securely as is practicable, the organisation ensures **[insert post procedures here]**.

5.3. *Portable devices*

The organisation is aware of the increased risk to information held on portable devices such as memory sticks, CDs, DVDs, etc. All portable devices have been documented on the Information Asset Register **[insert location here]**, and all relevant staff have received guidelines on safe usage and have signed an assignment of mobile computing equipment form.

Due to the increased risk of viruses and the risk of losing data, the following procedures are followed: **[Insert your procedures here, which may resemble the following:]**

i. Portable devices must be encrypted;

ii. Only portable devices issued by **[insert organisation name here]** may be used;

iii. Portable devices such as memory sticks, CDs, etc. must not be used on personal computers. **[delete if not relevant]**; and

iv. All portable devices are security marked

v. Password protected screensavers are installed on laptops;

vi. Anti-virus software **[name type]** is in use and is regularly updated **[insert how often]**;

vii. Regular backups are taken of the data stored on portable devices

5.4. *Faxes*

The fax machine is **[insert location here]** and when receiving faxes containing confidential information, the organisation ensures:

i. The fax is removed from the machine on receipt;

ii. Where necessary, the sender is contacted to confirm receipt;

iii. The information in the fax is appropriately dealt with and safely stored.

To ensure that confidential information transferred from the organisation by fax is done so as securely as is practicable, the organisation ensures:

i. The fax number is always double checked, and frequently used numbers are stored in the fax machine to reduce the risk of typing errors;

ii. A fax cover sheet is used and marked "Private and Confidential";

iii. Faxes are only sent to a named person rather than a team;

iv. The recipient is informed that a fax will be sent, and asked to confirm receipt;

v. Faxes are not sent outside a recipient organisation's working hours where there is no-one present to receive.

In addition, the organisation ensures that:

i. regular checks of date and time are performed, especially following power outages, or change of British summer time;

ii. journal logs are retained for **[insert number of years here]**;

iii. the fax machine is located in secure area.

[You should include the type of machine and any benefits it may have *i.e.* using a laser printer because the quality of print is better than an ink jet, if you use thermal paper it is worth identifying that it is susceptible to fading and becoming illegible.]

5.5. *Email*

[note that if your organisation does not have access to secure email, then your procedure should be to never send or receive sensitive personal information via email.]

The organisation is aware that person identifiable information (either of employees or service users) can only be sent by secure email *e.g.* NHSmail or similar. Both the recipient and sender must have access to secure email.

[In creating your policy around secure email, we recommend considering and incorporating NHSmail policies: https://digital.nhs.uk/nhsmail/policies. Should you have access to NHSmail, please note that there has been a policy change since 1st April 2017. The guidance on NHSmail usage have been

updated to reflect this: Sharing sensitive information guide for NHSmail; Encryption guide for senders; Encryption guide for recipients]

5.6. *Other forms of information exchange (e.g. text messages)*

[If your organisation uses other forms of information sharing please outline procedures here.]

6. Approval

6.1. These procedures have been approved by the undersigned and will be reviewed on an annual basis.

Name	
Date approved	
Review date	

[20] ICT Network Security Policy - Template

[This is a complicated policy which will not be relevant for many Care Providers, and for those for whom it is necessary you may find that your ICT Supplier/Support will be able to monitor, audit or otherwise check much of the procedures which are outlined below.]

1. Introduction

1.1. This document defines the Network Security Policy for **[insert organisation name here]** (hereafter referred to as "us", "we", or "our").

1.2. The Network Security Policy applies to all business functions and information contained on the network, the physical environment and relevant people who support the network.

2. Purpose

2.1. This document sets out our policy for the protection of the confidentiality, integrity and availability of the network, establishes responsibilities for network security and provides reference to documentation relevant to this policy.

3. Scope

[Identify the scope as is relevant to you.]

3.1. This policy applies to our networks which are used for:

i. The storage, sharing and transmission of non-clinical data and images;
ii. The storage, sharing and transmission of clinical data and images;
iii. Printing or scanning non-clinical or clinical data or images;

iv. The provision of Internet systems for receiving, sending and storing non-clinical or clinical data or images.

4. <u>The Policy</u>

4.1. **[Insert organisation name here]**'s information network will be available when needed, can be accessed only by legitimate users and will contain complete and accurate information.

4.2. The network must also be able to withstand or recover from threats to its availability, integrity and confidentiality. To satisfy this undertake to:

i. Protect all hardware, software and information assets under its control;

ii. Provide effective protection that is commensurate with the risks to its network assets;

iii. Implement the Network Security Policy in a consistent timely manner;

iv. To comply with all relevant legislation.

5. <u>Risk Assessment</u>

5.1. We will carry out security risk assessment(s) in relation to all the business processes covered by this policy. These risk assessments will cover all aspects of the network that are used to support those business processes.

5.2. The risk assessment will identify the appropriate security countermeasures necessary to protect against possible breaches in confidentiality, integrity and availability.

6. Physical & Environmental Security

6.1. Critical or sensitive network equipment will be housed in secure areas, protected by a secure perimeter, with appropriate security barriers and entry controls.

6.2. **[Insert job title here]** is responsible for ensuring that door lock codes are changed periodically, following a compromise of the code, if she/he suspects the code has been compromised, or when required to do so by the registered Caldicott Guardian/IG Lead **[delete as appropriate]**.

6.3. Critical or sensitive network equipment will be protected from power supply failures.

6.4. Critical or sensitive network equipment will be protected by intruder alarms and fire suppression systems.

6.5. Smoking, eating and drinking is forbidden in areas housing critical or sensitive network equipment.

6.6. **[Insert job title here]** is responsible for authorising all visitors to secure network areas and for making visitors aware of network security requirements.

6.7. All visitors to secure network areas must be logged in and out. The log will contain name, organisation, purpose of visit, date, and time in and out.

6.8. **[Insert job title here]** will ensure that all relevant staff are made aware of procedures for visitors and that visitors are escorted, when necessary.

7. Access Control to Secure Network Areas

7.1. Entry to secure areas housing critical or sensitive network equipment will be restricted to those whose job requires it.

7.2. **[Insert job title here]** will maintain and periodically review a list of those with unsupervised access.

8. Access Control to the Network

8.1. Access to the network will be via a secure log-on procedure, designed to minimise the opportunity for unauthorised access. Remote access to the network will conform to the Remote Access Policy.

9. Third Party Access Control to the Network

9.1. Third party access to the network will be based on a formal contract.

9.2. All third party access to the network must be logged.

10. External Network Connections

10.1. Ensure that all connections to external networks and systems have documented and approved System Security Policies.

10.2. **[Insert job title here]** must approve all connections to external networks and systems before they commence operation.

11. Maintenance Contracts

11.1. **[Insert job title here]** will ensure that maintenance contracts are maintained and periodically reviewed for all network equipment.

11.2. All contract details will constitute part of the Information Asset register **[insert IAR location here]**.

12. Data and Software Exchange

12.1. Formal agreements for the exchange of data and software between organisations must be established and approved by **[insert job title here]**

13. Fault Logging

13.1. **[Insert job title here]** is responsible for ensuring that a log of all faults on the network is maintained and reviewed. A written procedure to report faults and review countermeasures can be located **[insert location here]**.

14. Security Operating Procedures

14.1. Changes to operating procedures must be authorised by **[insert job title here]**.

15. Network Operating Procedures

15.1. Changes to operating procedures must be authorised by **[insert job title here]**.

16. Data Backup and Restoration

16.1. Data backup procedures are outlined in the Emergency and Business Continuity Plan document.

17. User Responsibilities, Awareness & Training

17.1. **[Insert organisation name here]** will ensure that all users of the network are provided with the necessary security guidance, awareness and where appropriate training to discharge their security responsibilities.

17.2. These procedures will be outlined in the staff handbook.

18. Accreditation of Network Systems

18.1. **[Insert job title here]** is responsible for ensuring that the network does not pose an unacceptable security risk to the organisation. They will require checks on, or an audit of, actual implementations based on approved security policies.

19. Malicious Software

19.1. Ensure that measures are in place to detect and protect the network from viruses and other malicious software.

20. Secure Disposal or Re-use of Equipment

20.1. Ensure that where equipment is being disposed of all data on the equipment (*e.g.* on hard disks or tapes) is securely overwritten.

21. System Change Control

21.1. **[Insert job title here]** is responsible for updating all relevant Network Security Policies, design documentation, security operating procedures and network operating procedures.

22. Reporting Security Incidents & Weaknesses

22.1. All potential security breaches must be investigated and reported to the IG Lead and an Information Security Incident Report Form must be completed.

23. Business Continuity & Disaster Recovery Plans

23.1. Ensure that business continuity plans are produced for the network.

23.2. The plans must be reviewed and tested on a regular basis.

24. Approval

24.1. These procedures have been approved by the undersigned and will be reviewed on an annual basis.

Name	
Date approved	
Review date	

[21] Records Management Policy & Procedures - Template

[note that the ICO has helpful advice on records management here: https://ico.org.uk/for-organisations/improve-your-practices/health-sector-resources/]

Records Management Policy

1. Introduction

1.1. Records Management is the process by which an organisation manages all aspects of records whether internally or externally generated and in any format or media type, from their creation, all the way through to their lifecycle to their eventual disposal.

2. Purpose

2.1. The Records Management Procedures set out how **[insert organisation name]** (hereafter referred to as "us", "we", or "our") will ensure that both service user & staff records are properly created, accessible and available for use and eventual disposal. They provide staff with guidance regarding individual responsibility for accuracy and appropriate storage of records.

3. Scope

3.1. These procedures relate to personal information held in any format by the organisation.

4. Creation of records

4.1. The principal purpose of service user records is to record and communicate information about the individual and their care. The principal purpose of staff records is to record employment details for payroll and business planning purposes.

4.2. To fulfil this purpose the organisation:

i. Uses standardised structures and layouts for the contents of records

ii. Ensures documentation reflects the continuum of care and is viewable in chronological order;

iii. Provides a clear written treatment plan when care/treatment is being delivered by several members of the team, and ensures records are maintained and updated, and shared with everyone involved;

iv. Implements a process that enables service users to have easy access to their records;

v. Provides guidance for staff on the creation and use of records (see staff handbook)

5. Retention of records

5.1. We have adopted the retention period for records set out in the Records Management NHS Code of Practice for Health and Social Care, which both state that the minimum retention period for health records is 8 years after treatment for adults, and for children until the service user's 25th birthday or 26th if young person was 17 at the conclusion of treatment, **or** 8 years after death.

5.2. We have adopted the retention period for staff records of **[insert number of years here]** years, including copies of contact details, appraisals and reviews.

5.3. We have adopted the retention period for our financial records of **[insert number of years here]** years from the end of the financial year in which they relate to.

5.4. The organisation will not apply to any records a shorter retention period than the minimum set out above.

5.5. The location of all records is recorded on the Information Asset Register (IAR).

6. Maintenance of service user records

6.1. The quality and the condition of the health record are vital to the service user and the organisation. Therefore, the organisation ensures that equipment used to store records on all types of media (paper or digital) is clean, safe and secure from unauthorised access or environmental damage and which meets health and safety and fire regulations, but which also allows maximum accessibility of the information proportionate to the frequency of use.

6.2. Hard-copy records that are in constant or regular use, or are likely to be needed quickly, are stored **[insert location here]** which comply with current Health and Safety regulations. The organisation ensures that the area containing health records is always locked when left unattended.

6.3. We have an archive storage facility **[insert location here]** that protects physical records from environmental damage, flooding, dampness and dust.

6.4. We ensure that digital records are subject to regular back-up and are regularly checked to ensure continuing access to readable information **[you may like to update this with your backup procedures here]**.

6.5. The location of all service user records is recorded on the IAR.

7. Use of records

7.1. Accurate recording and knowledge of the whereabouts of all records is crucial if the information they contain is to be located quickly and efficiently. To record transfers of hard-copy records we **[insert organisation procedure here]**.

7.2. We comply with the Common Law Duty of Confidentiality and ensure that staff members are provided with guidance on disclosures of service user information in its staff confidentiality code of conduct.

7.3. We have authorised the registered Caldicott Guardian/IG Lead **[delete as appropriate]** as the only person/people **[delete as appropriate]** permitted to disclose confidential information outside the organisation.

7.4. We ensure that when records are transferred or taken off-site it is in accordance with good Information Governance practice to ensure records are protected from unauthorised access or loss. We have implemented information handling procedures which are outlined in **[insert procedure document name here]**.

8. Disposal of records

8.1. Disposal encompasses archiving or destruction of the records. We appraise records that have reached their minimum retention period to decide whether or not a record is worthy of archival preservation, whether it needs to be retained for a longer period as it is still in use, or whether it should be destroyed.

8.2. Any documents identified as requiring permanent preservation are transferred to **[insert location here]**.

8.3. Where we decide that a record should be destroyed we ensure that destruction of health records is conducted in a secure manner by **[insert procedure here]**

8.4. We maintain a log of the disposal decisions taken regarding records.

9. Approval

9.1. These procedures have been approved by the undersigned and will be reviewed on an annual basis.

Name	
Date approved	
Review date	