[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.