Information Governance Reference Document

Introduction

Information Governance allows an organisation to manage its information in an efficient, effective and secure way whilst maintaining the balance between confidentiality and openness.

Information Governance processes allow this by ensuring:

- records are only kept for the appropriate period of time and that they are confidentially destroyed when no longer required.
- access to records is suitably managed and maintained so that requests for information can be dealt with in a timely manner.
- the appropriate privacy and security is applied to information and/or systems whilst in transit and storage.

Any organisation handling data, especially personal data, has a responsibility to ensure that it complies with Information Governance requirements.

This document intends to set out the responsibilities of all parties to ensure that everyone understands what is expected of them when handling data.

Section 1: Data Controller/Data Processor

All organisations handling personal data must comply with the requirements of the Data Protection Act 2018'. In addition to this, a Data Processor must also comply with any obligations imposed upon it by the Data Controller.

Data Controller – The responsible party for personal data who determines the purposes for which and the manner in which any personal data are, or are to be, processed.	**Data Processor** – is any person (other than an employee of the Data Controller) who processes data on behalf of the Data Controller.

Community Managed Libraries (CML) will have access to personal and sensitive personal data. Some of this data will belong to the Council but the CML will need access to in order to provide the Library service. For example Library user data will belong to the Council, however volunteer data will belong to the CML.

Where data belongs to the Council, the Council will be the Data Controller and the CML will be the Data Processor. Where the data belongs to the CML, the CML will be the Data Controller.

Some examples of the division of data are included below (this is not an exhaustive list):

Data belonging to SCC	Data belonging to CML
Data pertaining to Library users	Data pertaining to volunteers working for the CML
CCTV footage	
Leasing documentation	

On occasion SCC will need access to data which is held by the CMLs. When this occurs the relevant CML will be required to provide the records to SCC in the required format in the timescales requested.

If the CML organisation ceases to provide the library service then all data in possession of the CML must be returned to SCC. SCC will become the data controller for this data when it is transferred. SCC will then be solely responsible for any subsequent decisions in relation to processing the transferred data, including retention and secure destruction.

Section 2: Volunteers

The CML will be responsible for appointing and training Library volunteers. As these volunteers may require access to data owned by the County Council they will be required to sign a volunteer agreement (Appendix A) to confirm that:

- They have received appropriate training regarding handling data and their responsibilities relating to Data Protection, Confidentiality and Information Security.

- They have read and understood the County Council's Information Security Policy (Appendix B).

- They have read, understood and signed the County Council's Acceptable Use Policy (Appendix C).

- They have been made aware of, and work in line with, this Information Governance Reference Document.

- They understand that the County Council reserves the right to restrict or remove access to data and/or systems where non-compliance is evident or where a threat, or potential threat, is identified. Where illegal or criminal behaviour is suspected or identified SCC will refer the matter to the Police.

Third Party Access Agreements must be signed by each CML volunteer who requires access to SCC systems, for example the Library Management Systems. Third parties are defined as anyone who are not directly employed by SCC. Access to systems will not be provided unless these forms and the Volunteer Agreement are completed.

Section 3: Managing Information

Library volunteers will need to ensure that SCC data is only accessed when required and that it is accessed only by those volunteers who are authorised to access it.

All Library volunteers will require access to the Library Management Systems in order to carry out their roles. They will require access to service users personal data in order to process bookings, manage current (including update personal data where required) and sign up new members accounts, ensure stock and bank elements are maintained.

All Library volunteers will ensure that any data they record has a specific purpose for recording and that data recorded is not excessive. When recording data volunteers should ensure that the data is accurate and up to date, as far as reasonably possible.

In order to be provided access to the system and SCC networks (if applicable) volunteers must sign the Acceptable Use Policy, Volunteer Agreement and have completed relevant training pertaining to Information Governance and their role.

Manual records belonging to SCC must be maintained and destroyed when applicable in line with SCC retention schedules to ensure compliance with the Data Protection Act. Retention Schedules can be found on the SCC Intranet.

Section 4: Access to Information

a. Freedom of Information requests

As a Public Body, the County Council has a legal obligation to be open and transparent regarding the way in which it manages its services. Information in the public interest should proactively be made available and requests for information must be handled in line with statutory requirements.

Where a written request for information is made regarding the Library service the County Council will respond accordingly. The CML may be required to provide reasonable assistance to the Council in order for us to meet our legal obligations. This includes providing records relating to requests as directed by the Council and within given timescales.

Where a written FOI request is received by a CML your Community Support Officer should also be informed and the request must be sent to the Information Governance Unit within 2 working days. The email address to be used is foi@staffordshire.gov.uk

b. Data Protection request (Subject Access)

Where service users request information for which SCC is the Data Controller, SCC will be responsible for managing and responding to these requests. If a request for SCC personal data, i.e. Library user data is made to the CML, they must forward that request to SCC Library services within 2 working days who should pass this on to the Information Governance Unit.

The CML will be responsible for handling Data Protection requests relating to personal data for which they are the Data Controller.

c. Request for information from third party organisations

On occasion it may be necessary for a Data Controller to share personal data with other organisations where it is necessary, justified and proportionate to do so. Decisions to share personal data with third parties can only be taken by the Data Controller therefore any request made to a CML for data owned by SCC must be transferred to the SCC Library services who should pass this on to the Information Governance Unit. For example a request from a third party organisation may be a Police request for CCTV or for service user information.

The CML will be responsible for taking decisions about disclosures relating to personal data for which they are the Data Controller.

Section 5: Information security

Manual and electronic data owned by SCC must be held securely and appropriate technical and organisational measures must be put in to place by the CML to ensure this. For example hardcopy records containing personal data should be held in a lockable cupboard/cabinet.

Library volunteers will need to ensure that SCC data is only accessed when required and that it is accessed only by those volunteers who are authorised to access it.

If the CML believes that a security incident has occurred relating to data belonging to SCC, the CML must contact the Library services within 2 working days of the security incident being discovered. Library services must pass this on to the Information Governance Unit using the SCC information security incident reporting process.

Section 6: Public Wi-Fi and computers

a. Public access to Wi-Fi

The County Council will be responsible for ensuring that free Wi-Fi is available for public access in CML.

When users attempt to log on to the County Councils Wi-Fi they will be required to read and accept a short electronic disclaimer. This highlights, amongst other things, that the guest wireless network is unsecured and information sent over the network may be visible to others. If the network is used for confidential information it is done at the users own risk and the Council is not liable for any losses that may occur.

b. Public access computer

The County Council will lease at least one computer to the CML for public access.

The CML must ensure that all users of these computers adhere to the following criteria:

In order for service users to use the public access computer provided by SCC they must first be registered with the Library and then sign the Acceptable Use Policy before access will be granted. For requesters who are 16 years old and below the Acceptable Use Policy is sent out by post to a parent to be signed.

PINs are generated and assigned by one of the Library Management Systems to users in order for them to access the PCs. Library volunteers would be expected to manage any queries or issues that arise in relation to accessing PCs and to issue users with PINs when required.

Any issues arising from access to SCC systems/networks/computers should be reported to your Community Support Officer.

Staffordshire Libraries – Volunteer Agreement

Confidentiality Statement

In undertaking the agreed duties for which I am authorised as a library volunteer, I agree to the following statements:

1. I have received appropriate training regarding handling of information and am aware of my obligations and responsibilities relating to, but not limited to, Data Protection, Confidentiality and Information Security

2. I have read and understood Staffordshire County Council's Information Security Policy

3. I have read, understood and signed a copy of Staffordshire County Council's Acceptable Use Policy

4. I have been made aware of, and understand that I must work in line with, the Information Governance Reference Document

5. I understand that Staffordshire County Council reserve the right to restrict or remove access to data and/or systems where failure to comply with the above is established or where any threat or potential threat is identified

6. I understand if I need to take identifiable information offsite only in the course of my volunteer role that it must be kept secure. I will never leave documents with personal data unattended at any point unless they are locked away and secure

7. If, for whatever reason, my volunteer role ends I understand my ICT access will be revoked and I must not remove any data used in my role as it remains property of the organisation

Volunteer name: _____

Volunteer signature: _____

Library: _____

Date: _____

Appendix B

Corporate Information Security I

Appendix C

Acceptable Use Policy 2015.pdf