Information Security Policy

This policy was agreed by the Trust Board on 19 December 2017 to be used as an interim policy by Sandwell Children's Trust.

The intention is to review this policy by 1 July 2018 to ensure that it is fit for purpose for the Trust.

Sandwell
Children's Trust

Information Management Unit

Information Security Policy

Document Type: Tier 1 Policy

Version: 1-0 FINAL

Date Issued: 2014

Document Control

Owning organisation	Sandwell Council
Title	Information Security Policy
Author	James Trickett
Protective Marking	IL0: UNCLASSIFIED
Review Date	May 2016

Revision History

Revision Date	**Editor**	**Previous Version**	**Description of Revision**
23rd April 2014	James Trickett	n/a	Final version

Document Distribution

Please note – once printed, this documented is uncontrolled. The latest version will always be found on the Council's intranet.

Document Approvals

Approval required	**Date approved**
JCP	25th March 2014
Leader Decision Making Session	23rd April 2014

Contents

1.0 Introduction

1.1 Information is an asset. Like any other business asset it has a value and must be protected. Systems that enable us to store, process and communicate this information must also be protected in order to safeguard information assets. ‘Information systems’ is the collective term for our information and the systems we use to store, process and communicate it. Information systems include paper / manual and / or electronic / computer systems.

1.2 This policy is part of a set of information governance policies, Codes of Practice and procedures that supports the delivery of the Information Governance Framework. It should be read in conjunction with these associated policies.

1.3 Information security is an integral part of information sharing, which is becoming increasingly important to achieving council aims and objectives – especially when joint working with sectors such as health.

1.4 The purpose of our Information Security Policy is to protect the Council’s information, manage information risk and reduce it to an acceptable level, while facilitating reasonable use of information in supporting normal business activity and that of our partners.

1.5 Information Security involves the protection of information and we are committed to preserving the confidentiality, integrity and availability of our information assets:

- For sound decision-making;
- To deliver quality front line services;
- To comply with the law;
- To meet the expectations of our service users and partners;
- To protect our reputation as a professional and trustworthy organisation.

1.6 This Policy has been developed using the internationally recognised standard for information security known as

ISO27001. This takes a risk based approach to upholding the 3 key principles of information security:

- Confidentiality
- Integrity
- Availability

1.7 Information is a generic term used throughout this Policy. It can take many forms e.g. electronic, written or vocal. It would be wrong to assume that information in any form warrants the highest level of protection or may never be disclosed as described in this Policy. Local Authorities, like Central Government, are advised to adopt the Government's Protective Marking Scheme which classifies information dependent on its attributes e.g. most people are familiar with the term 'confidential' which is one of the 6 markings available. The Government's protective marking system is designed to help individuals determine, and indicate to others, the levels of protection required to help prevent the compromise of valuable or sensitive assets. The markings signal quickly and unambiguously, the value of an asset and the level of protection it needs.

1.8 Therefore in applying this Policy everyone handling information must take a pragmatic and sensible approach e.g. a publically available newspaper or leaflet does not warrant anything near the same protection as an extract from the Child Protection Register and therefore the rules of not keeping it on an unattended desk would be absurd. However the adoption of a clear desk policy helps to mitigate against this risk

1.9 Therefore common sense and professional judgement must be applied taking into account other demands such as the Freedom of Information Act. For the avoidance of doubt, other supporting resources and contacts are available as described throughout this Policy.

2.0 Scope and Definition

2.1 Information security is defined as safeguarding information from unauthorised access or modification to ensure its:

- **Confidentiality** – ensuring that the information is accessible only to those who have access;
- **Integrity** – safeguarding the accuracy and completeness of information by protecting against unauthorised modification;
- **Availability** – ensuring that authorised user have access to information and associated assets where required.

2.2 This policy applies to everyone who has access to the council's information, information assets or ICT equipment. These people are referred to as 'users' in this policy. This may include, but is not limited to employees of the council, members of the council, temporary workers, partners and contractual third parties.

2.3 The Information Security Policy applies to information in all its forms, including, but not limited to:

- Paper
- Electronic Documents
- E-mails
- Text messages
- Blogs, social media and discussion groups
- Visual images such as photographs and video
- Scanned images
- Microfiche and microfilm
- Published web content – internet and intranet
- Audio and video recordings
- Databases

2.4 Users of Council's information assets will abide by UK and European legislation relevant to information security including:

- Data Protection Act 1998
- Freedom of Information Act 2000
- Computer Misuse Act 1990
- Electronic Communications Act 2000
- Copyright, Designs and Patents Act 1988
- Human Rights Act 1998

- Regulation of Investigatory Powers Act 2000
- Telecommunications (Lawful Business Practice) Regulations 2000
- Civil Contingencies Act 2004

This list is not exhaustive and may change over time.

2.5 This policy will also apply to any information created in any other format that may be introduced or used in the future.

2.6 The policy includes information transmitted by post, by person, by electronic means and by verbal communication, including telephone.

2.7 The policy applies throughout the lifecycle of the information from creation, utilisation, storage and to its ultimate disposal.

2.8 With regard to electronic information systems, it applies to use of council owned facilities and privately/externally owned systems when connected to the council network directly or indirectly.

2.9 Information belonging to third party and partner organisations will be handled and processed in line with this policy and in accordance with any requirements set out by the third party which may include Information Sharing Protocols (ISPs) or a Memorandum of Understanding (MoU).

3.0 Roles and Responsibilities

3.1 The Council's Senior Information Risk Officer (SIRO) has responsibility for managing information risk on behalf of the Chief Executive and Senior Management Board, setting strategic direction and ensuring policies and processes are in place for the safe management of information.

3.2 Directors have responsibility for understanding and addressing information risk within their service areas, assigning ownership to Information Asset / System Owners and ensuring that within their directorate appropriate arrangements are in place to manage information risk, and to provide assurance on the security and use of those assets.

3.3 Information Asset / System Owners undertake information risk assessments, implement appropriate controls, recognise actual or potential security incidents and ensure that policies and procedures are followed.

4.0 Key policy purposes

4.1 The purpose of the policy is to provide a framework giving guidance for the establishment of standards, baselines, sub-policies, procedures and guidelines for implementing information security and reinforce the council's commitment to ensuring that its information assets are protected and secure.

4.2 It aims to:

- Demonstrate assurance of the confidentiality, integrity and availability of information held or processed by the Council;

- Ensure that information risks are identified and managed appropriately;

- Minimise the business impact and interruption caused by security incidents;

- Ensure that all information and information systems upon which the council depends are designed and protected with security applied to the required standards;

- Ensure that all users are made aware of their obligations and have a proper awareness, concern and an adequate appreciation of their responsibilities for information security and take appropriate measures to avoid loss, misappropriation or misuse of information;

- Ensure that all users have an awareness of their responsibilities for processing personal information or any other information of commercial value;

- To ensure that any sharing of information is lawful, properly controlled and the data protection rights of individuals are respected;

- Ensure that all contractors and their employees, temporary workers and other visitors likely to use and process council information have a proper awareness and concern for the security of council information;

- Meet the general objectives and support the principles of:

    - Cabinet Office Security Policy Framework (SPF);
    - ISO27001, International Standard on Information Security Management Systems (ISMS);
    - Payment Card Industry Data Security Standards (PCI-DSS);
    - Code of connection for the Public Sector Network (PSN);
    - Information Assurance Maturity Model;
    - LGA Data Handling Guidelines, and
    - NHS Information Governance toolkit.

5.0 Key Security Principles

5.1 The information lifecycle which is the creation, storage, maintenance, retention, sharing and disposal processes should comply with the following principles of information security:

- Measures taken or installed are appropriate to the level of security required to maintain the confidentiality, integrity and availability of information;

- Appropriate technical controls shall be implemented to ensure the protection and management of all electronic information;

- Users should take appropriate measures to prevent unlawful or unauthorised disclosure of information;

- Users should take appropriate measures to prevent accidental or malicious alteration or deletion of information;

- Users should be able to access information for the effective performance of their role;

- Access to information should be on a 'need to know' basis;

- Users will only be given access privileges which are absolutely essential to do their work i.e. principle of least privilege;

- Users must consider if they have now, in the past or in the foreseeable future, any possible conflicts of interest relating to the information they are accessing and, if so, should alert their line manager who must ensure there is a clear segregation of duties;

- Information security should not create a barrier to the flow of information across the council, but should provide appropriate controls and permissions;

- Users are accountable for their use of information, information assets and ICT equipment;

- Information security processes must comply with prevailing legislation e.g. Data Protection Act, Freedom of Information Act;

- All Information in any format must be assigned and marked with an appropriate classification in accordance with the Information Classification Scheme;

- Data backup and recovery and business continuity plans are tested and maintained to ensure that vital information services are available within defined service levels;

- Breaches of information security controls will be reported to and will be investigated by an officer who has been assigned information compliance responsibilities;

- Users will not copy software or licensed products without the permission of the owner of the copyright (under some circumstances such copying may be a breach of the Copyright, Designs and Patents Act 1988;

- Users will consider security when using and disposing of information and should:

  - Refer to the Council's guidance and procedures related to retention and disposal;

  - Ensure that all information is covered by an appropriate retention period;

  - Follow established procedures for the safe and secure disposal of information safely;

5.2 All council computer hardware must be disposed of in accordance with Council guidance and procedures;

5.3 Users must take appropriate measures to prevent problems with data quality.

6.0 Information Security Requirements

6.1 Sandwell Council has a significant investment in ICT and information. The Council is dependent upon the information it holds and processes. The incorrect disclosure or loss of information or loss of its ICT processing facilities could lead to significant additional costs, loss of revenue and damage to the Council's reputation as a result of:

- Business activities being fully or partially suspended (if the information is personal data, formal intervention from the Information Commissioner);
- Having to recover information or ICT facilities and equipment;
- Unauthorised disclosure of protected information relating to individuals being made available to 'interested parties';

- Vulnerable citizens being put at risk as a result of key information not being available to the people who need it or being disclosed inappropriately;
- Fraudulent manipulation of cash or goods.

Always remember:

- Information Security is your personal responsibility. All information will have an owner or author. Know the rules for handling the information in your care. Stick to those rules without exception;
- Before making information available to anyone else, make certain you have the authority, including the legal power, to release it;
- Never access information unless it is part of your job and you have a business need to do so;
- Never give out information via the telephone or in any other way unless you are absolutely sure who you are giving it to, that it is adequately protected whilst in 'transit' and that the recipient is entitled to receive it;
- Remember - always take reasonable and practicable steps to protect the information you store or process;
- Ensure data transfers are undertaken lawfully and legitimately using the correct tools and processes at all times;
- Do not disclose any details pertaining to the Council's security systems or processes – take particular care of "social engineering" where this method maybe used to probe for weaknesses and hence launch some form of attack on our systems.

When in the office:

- Never leave information out on your desk when you are not present;
- Adopt the clear desk policy;
- Always 'lock' your computer or smart phone before leaving your desk or the device unattended;
- Lock and remove the keys from cabinets or other storage units if you leave the office unattended – during the daytime or out of hours;
- Choose your passwords carefully and never let anyone else know them;

- Challenge anyone you see in the building who should not be there – do not allow anyone to ‘tail gate’ you through security doors.

On the move:

- Never take information out of the office unless you need to;
- Keep your ICT equipment – laptops, telephone, smart phone and paperwork secure at all times;
- Never leave equipment, information or documents in a vehicle when it is unattended and always travel with it locked securely and out of sight e.g. in the boot;
- When working in a public place, make sure you are not overheard and that information cannot be seen by others;
- Take care when using public or free networks – these may not be secure and data may be intercepted;
- When agile working ensure you take account of all the appropriate guidance – this is equally important when working at home as in a Council office.

Transmitting information:

- Ensure the information is being sent / transmitted to the correct person / destination;
- Always make sure you know what Protective Marking or sensitivity the information you are using should have and always comply with that level of protection;
- Be certain you are sending only what you absolutely need to send and no more;
- Ensure the method of transfer is appropriate to the protection of that information and if in any doubt do not use it e.g. use of provided encryption tools whenever available;
- Data Processing Agreements and /or Protocols must be in place for any information transferred to a third party and the Council remains as the recognised Data Processor;
- Undertake Privacy Impact Assessments where necessary.

7.0 Training

7.1 Appropriate training will be made available for new and existing staff who have responsibility for information governance duties;

7.2 All users will be made aware of their obligations for information governance through effective communication programmes;

7.3 Each new employee will be made aware of their obligations for information governance during their induction programme;

7.4 Training requirements will be reviewed on a regular basis to take account of the needs of the individual, and to ensure that users are adequately trained.

8.0 Policy Compliance and Audit

8.1 Failure to observe the requirements set out in this policy may be regarded as serious and any breach may render an employee liable to action under the council's disciplinary procedure.

8.2 Non-compliance with this policy could have a significant effect on the efficient operation of the Council and may result in financial loss and an inability to provide necessary services to our service users. The Council will undertake audits as required to monitor compliance with its information governance policies and, where necessary, will monitor users' access to information for the purpose of detecting breaches of this policy and/or other information governance policies and procedures.

8.3 It is the duty of all users to report, as soon as practicably possible, any actual or suspected breaches in information security in accordance with the procedures outlined on the Information Management Unit intranet.

8.4 Any user who does not understand the implications of this policy or how it may apply to them, should seek advice from their immediate line manager and/or the Information Management Unit.

9.0 Information Security Policy Exemptions

9.1 Exceptions will be granted only where there is a clear business case to do so, and where there is evidence that a risk assessment has been undertaken and any additional risks introduced by the exception are mitigated to an acceptable level. The approval of the relevant Director is required, along with the approval of the Information Management Unit.

End of document