Information Security Policy

Wiltshire Council

Where everybody matters

Document Control

Reference Number	**Version** 2.0	**Status** Published	**Sponsor(s)/Author(s)** Tim Way, Sarah Davis-Solan
Amendments	2.0 Regular review 2.1 updated links to NHS/DSP toolkit and DP to GDPR		
Document objectives: To establish high level security policy for the protection of all information held by the council to maintain its confidentiality, integrity and availability			
Intended Recipients: None			
Group/Persons Consulted: None			
Monitoring Arrangements and Indicators: None			
Training/Resource Implications:			
Ratifying Body and Date Ratified	Information Governance Programme Board September 2019		
Date of Issue	February 2019		
Review Date	February 2020		
Contact for Review	Information Governance		
SIRO signature			

Associated Documentation

Wiltshire Council policies

- Information Governance Policy
- Information Governance Management Framework
- Network Security Policy
- Mobile Working Policy
- Information Asset System Change Policy
- System Level Security Policy
- Information Incident Management Policy
- Records Management Policy
- Information Asset Policy

Legal framework

- Computer Misuse Act 1990
- Copyright Design and Patents Act 1988
- The General Data Protection Regulation 2018
- Freedom of Information Act 2000
- Health and Safety at Work Act 1974
- Regulation of Investigatory Powers Act 2000

Codes of Practice and Guidance

- ISO 27000-2013 document series
- NHS IG Toolkit / DSP Toolkit

  Cyber Essentials https://www.gov.uk/government/publications/cyber-essentials-scheme-overview
- PSN Code of Connection (CoCo) https://www.gov.uk/guidance/apply-for-a-public-services-network-psn-connection-compliance-certificate
- Government End User Device Security and Configuration Guidance https://www.gov.uk/government/collections/end-user-devices-security-guidance
- Payment Card Industry Data Security Standards PCI-DSS https://www.pcisecuritystandards.org/

Contents

1. Executive Summary

The objective of information security is to ensure confidentiality, integrity and availability of information assets, whilst minimising business damage through the implementation of standards, controls and procedures, which support the policy. This includes cyber-security and implementation of the ‘Cyber Essentials’ framework.

The purpose of the policy is to safeguard Wiltshire Council’s (the council’s) corporate and personal information and the personal information of council Service Users within a secure environment.

The council’s Senior Information Risk Officer (SIRO) and those with delegated responsibility for information security have approved and support this policy.

It is the policy of the council to ensure that:

- Information will be protected and controlled against unauthorised access or misuse;
- Confidentiality and integrity of information will be assured;
- Business Continuity Planning and ICT Disaster Recovery processes will be maintained;
- Regulatory, contractual and legal requirements will be complied with;
- Regular Information Governance training will be provided for all staff;
- Information assets will be identified, classified, risk assessed and protected as required, by those who have been identified as responsible for them on behalf of the organisation;
- Physical, logical, environmental and communications security will be maintained;
- Operational procedures and responsibilities will be maintained;
- All breaches of information security and confidentiality will be reported and investigated;
- Infringement of the policy may result in immediate disciplinary action or criminal proceedings;
- Standards and procedures will be produced and measures implemented to support the policy;
- Business requirements for the availability of information and information systems will be met, and information will be available to those who need to use it on behalf of the council;
- The SIRO has overall responsibility for the maintenance and implementation of the policy.

2. Introduction

Information is one of the council’s most important assets. The council and its staff have responsibilities and legal requirements to keep information safe, secure and confidential. Particular care must be taken with customer, client and staff identifiable information.

Failure may open the council to criticism or legal action or both. The confidence of the public in the council may be compromised if information is not kept safe and secure.

This policy is intended to inform all staff of their responsibilities and help them meet these requirements. This policy refers to standards, policies and procedures as well as legal guidance which are used to develop and support proper systems of keeping information secure and confidential.

3. Objective

The objectives of the council Information Security Policy are to preserve:

- Confidentiality: access to data must be restricted to those with specific authority to view the data;
- Integrity: Information is to be complete and accurate. All systems, assets and networks must operate correctly, according to specification;
- Availability: information must be available and delivered to the right person, at the right time.

4. Aim

The aim of this policy is to establish and maintain security and confidentiality of information, information systems, applications and networks owned or held by the council, by:

- Ensuring that all members of staff are aware of, and fully comply with, the relevant legislation as described in this and other policies;
- Describing the principles of security and explaining how they will be implemented in the council;
- Introducing a consistent approach to security, ensuring that all members of staff fully understand their own responsibilities;
- Creating and maintaining within the council a level of awareness of the need for Information Security as an integral part of the day to day business;
- Protecting information assets under the control of the council.

5. Scope

The policy applies to all data and access to data.

The policy applies to all those having access to information such as staff employed by the council; to those engaged in duties for the council under a Letter of Authority, Honorary Contract or Work Experience programme; and any other third - party such as contractors, students or visitors.

6. Legislation

The council is obliged to abide by all relevant UK and European Union legislation. The requirement to comply with this legislation will be devolved to employees and agents of the council, who may be held personally accountable for any breaches of security for which they may be held responsible. The council will comply with the legislation as appropriate.

In meeting the requirements to comply with legislation the council will issue appropriate policies, procedures and guidance.

7. Responsibilities for Security

Ultimate responsibility for security rests with the SIRO.

The Information Security Policy shall be maintained, reviewed and updated by the Information Governance (IG) Manager. This review shall take place annually or when changes are required. The IG Manager is responsible for assuring compliance and collating / reporting exceptions to the Information Security Policy and supporting practices and procedures.

The Head of ICT is responsible for defining, documenting and operationally maintaining practices and procedures to implement Information Security technical controls.

Information Asset Owners(IAO) and Line Managers are responsible for ensuring that their permanent and temporary staff and contractors are aware of:

- The information security policies applicable in their work areas;
- Their personal responsibilities for information security;
- How to access advice on information security matters;
- All staff must comply with security procedures, including the maintenance of data confidentiality and data integrity. Failure to do so may result in disciplinary action;
- All staff shall be individually responsible for the security of their physical environments;
- Each user shall be responsible for the operational security of the information systems they use: e.g. using passwords and logging on and off;

- Each system user must comply with the security requirements that are currently in force, and must also ensure that the confidentiality, integrity and availability of the information they use is maintained to the highest standard;
- Contracts with external contractors that allow access to the council's information systems will be in operation. These contracts will ensure that the staff or sub-contractors of the external organisation will comply with all appropriate security policies.

8. Policy Framework

8.1 Management of Security

At board level, responsibility for Information Security will reside with the SIRO.

The council's IG Manager will be responsible for documenting monitoring and communicating information security requirements for the council.

The Head of ICT will be responsible for the operational implementation of solutions, practices and supporting procedures which meet Information Security Policy requirements.

8.2 Information Security Awareness Training

Information security awareness training will be included in the staff induction process. An on-going awareness programme will be established to ensure that staff awareness is kept up-to-date.

8.3 Contracts of Employment

Security requirements will be addressed at the recruitment stage and all contracts of employment will contain confidentiality, information security and data protection clauses, including that of temporary staff. Security requirements will be included in job definitions where required.

8.4 Security Vetting

Security vetting is required for some job roles and before access is granted to certain sensitive information systems and data. The requirement for security vetting for these systems will apply to volunteers, partners and third parties as well as staff.

8.5 Security Control of Assets

IAOs will be responsible for the security of information assets in their service.

8.6 Physical Access Controls

Only authorised personnel, who have an identified need, will be given access to restricted areas.

8.7 User Access Controls

Access to information will be subject to individual identification and authentication, and will be restricted to authorised users who have an identified need to access the information.

User Accounts and associated access rights will be amended or removed following the Staff Movers and Leavers process. Minimum access rights required to meet business need will be granted. Access rights will be subject to periodic review by Information Asset Owners in conjunction with Head of ICT.

8.8 Computer Access Control

Access to computer facilities will be subject to individual identification and authentication and restricted to authorised users who have an agreed.

8.9 Application Access Control

Access to data, system utilities and program source libraries will be controlled through individual identification and authentication, and restricted to authorised users. Authorisation to use an application will depend on the availability of a licence from the supplier.

8.10 Equipment Security

To minimise loss of, or damage to hardware assets and the information they store, equipment will be physically protected from security threats and environmental hazards.

8.11 Computer and Network Procedures

Management of computers and networks will be controlled by documented procedures and practices that have been approved by the Head of ICT and authorised by the IG Board and the SIRO.

8.12 Secure Configuration

Information systems and supporting technical infrastructure will be designed, configured, built and tested using best practice secure configuration standards.

Approval of configurations will be by the Head of ICT in consultation with the IG Manager. All configurations of hardware and software will be subject to periodic penetration testing by independent ethical hacking organisations.

8.13 Security Incidents and weaknesses

All information security incidents, (including Data Leakage/Loss Incidents and Cyber Security concerns) must be reported to IG using the Incident Reporting Form. All IT related incidents or weaknesses, (loss of laptop, tablet, Smartphone or suspected phishing virus infection) should be reported initially to the ICT Service Desk.

ICT will identify cyber security incidents through monitoring system logs for unauthorised access attempts, unauthorised system changes and unusual system responses. All information security incidents will be recorded and investigated to establish their cause, operational impact, reporting requirements and response.

8.14 Protection from Malicious Software

The council will use software countermeasures and management procedures to protect itself against the effects of malicious software.

Unsupported versions of software will only be used by exception, recorded and approved by Head of ICT and IG Manager. All staff will be expected to co-operate fully with this requirement.

8.15 Software or Data from External Sources

Software or data from external sources, or which have been used in external equipment, must be fully virus checked and assessed for threats before being used on the council's equipment. Anyone breaching this requirement may be subject to disciplinary action.

8.16 Monitoring System Access and Use

An audit trail of system access and use will be maintained and reviewed to permit forensic investigation in support of Incidents. Audit logs will be retained in compliance with regulatory obligations and legislation.

8.17 Accreditation of Information Systems

The council will ensure that all new information systems, applications and networks include an information security risk assessment and mitigating actions plan approved by the IG Manager before implementation.

8.18 System Change Control

Changes to information systems, applications or networks must be reviewed and approved under the Information Asset Change Policy or by the ICT Change Management Process, whichever is proportionate for the impact of the change.

8.19 Intellectual Property Rights

The Head of ICT will ensure that all information software products are properly licensed. Only authorised systems can be used and only authorised users may install commercial software on the council's hardware assets. Users must not install commercial or copyright software without permission. Anyone breaching this requirement may be subject to disciplinary action.

8.20 Business Continuity and Disaster Recovery Plans

IAOs, in conjunction with Head of ICT and Head of Public Protection and Resilience, will ensure that business continuity and disaster recovery plans are produced for all critical information, applications, systems and networks. Solutions must be implemented which meet service availability requirements.

8.21 Reporting

The Head of ICT will provide regular and ad hoc data to the IG Manager to indicate the effectiveness of technical security control measures. The IG Manager will keep the IG Board informed of the information security status of the council by means of regular reports.