Corporate Information Security Policy

Document Management

Document Disclaimer

This document is issued only for the purpose for which it is supplied.

Document Owner

This document is produced and owned by Staffordshire County Council (SCC). It is the responsibility of the Information Security Team to review and update annually and as required.

Document Control

This document is controlled and maintained according to the documentation standards and procedures of Staffordshire County Council. All requests for changes to this document must be sent to the Information Security Team.

Distribution List

This document is published on the intranet for access by all users and will be sent to the recipients as defined within the distribution list maintained by the Information Security team.

Copy	Name
1	SICT Senior Management Team

Change History

Version	Author (s)	Reason for Change	Date
0.1	C Whitehouse	Initial policy	April 02
0.2	D Sharkey, M Dhami	Revision to reflect new SICT organisation and technology developments	May 05
0.3	D Sharkey, M Dhami	Revised daft incorporating comments.	August 05
0.4	Pat Yates	Updated amendments and format	October 05
0.5	Pat Yates	Updated version	February 2006
0.6	Pat Yates	Updated with Information Security Forum comments	August 2006
0.7	David Sharkey	Updated with external audit comments	August 2008
0.8	David Sharkey	Updated version	May 2014
0.9	IGT	Review	August 2016

Approvals

Version	Name	Position	Date Approved
0.1	Directors Board		May 2002
0.6	SICT Operations Board		November 2007
0.7	Corporate Governance Group		August 2008
0.8	Corporate Governance Group		May 2014
0.9	Corporate Governance Group		November 2016

Contents

1. Introduction

The Information Security Policy provides direction and support for information security in line with business requirements and relevant laws and regulations. The objective of information security is to:

- Protect the information assets of the County Council and any shared assets of partners;

- Ensure business continuity and minimise business damage by preventing and minimising the impact of security incidents.

The Council depends on the data which is stored and processed on its computers and the management information generated from the data. Effective information security is a team effort, which requires all users who deal with information and information systems to actively support and participate.

Information Security is defined as the preservation of:

- **Confidentiality:** ensuring that information is accessible only by those authorised to have access;

- **Integrity:** safeguarding the accuracy and completeness of information and processing methods;

- **Availability:** ensuring that authorised users have access to information and associated assets when required.

Preserving confidentiality, integrity and availability applies not just to information held electronically, but also to paper, microfiche and other media essential to the Council. Losing data and computing processing facilities or breaching access guidelines is likely to result in significant costs, a loss of revenue, damage to the Council's reputation or result in a fine of up to £500,000 from the Information Commissioners Office (ICO). Information security is achieved by putting in place a suitable set of policies and procedures that all users must adhere to. This policy is relevant for anyone who has access to the Council's ICT facilities including Members, staff and other users.

2. Scope

This Security Policy sets out specifically what responsibilities management and users have to maintain effective security mechanisms. It will also help the County Council in complying with appropriate legislations. These include but are not limited to Data Protection Act (1998), Computer Misuse Act (1990), Copyright Designs and Patents Act 1988 and the Freedom of Information Act (2000).

This policy identifies how the County Council will secure all data and follow the code of practice for information security set out in ISO/IEC 27002: 2013. The policy will be reviewed annually by the ICT Security Management Team to make sure it remains relevant and reflects how risks are managed.

Information Security in schools is not addressed in this policy. Instead we have developed separate guidance for individual schools which can be used to develop a policy suited to their local requirements.

3. Responsibilities

Objective: To ensure that all authorized users with access to the Council's ICT facilities are aware of their responsibilities and the commitments required in order to comply with the policy.

Security is everybody's business and therefore it is everybody's responsibility.

Senior Information Risk Officers (SIROs) must:

- Oversee the compliance with Information Governance (IG) Framework IG policies, standards and methods.

- Take ownership of the assessment processes for information risk, including prioritisation of risks and review of the annual information risk assessment to support and inform the Annual Information Governance Statement.

- Ensure that the Corporate Governance Working Group are kept up to date and briefed on all information risk issues affecting the organisation and its business partners.

- Review and agree actions in respect of identified information risks.

- Ensure that the organisation's approach to information risk is effective in terms of resource, commitment and execution, being appropriately communicated to all staff.

- Provide a focal point for the escalation, resolution and/or discussion of information risk issues.

- Ensure that an effective infrastructure is in place to support the role by developing a simple Information Assurance governance structure, with clear lines of Information Asset ownership and reporting with well-defined roles and responsibilities.

- Ensure that identified information threats and vulnerabilities are followed up for risk mitigation, and that perceived or actual information incidents are managed in accordance with SCC IG requirements.

- Ensure that there are effective mechanisms in place for reporting and managing incidents relating to the information of the organisation. These mechanisms should accommodate technical, operational or procedural improvements arising from lessons learnt.

- Provide leadership for the Information Asset Owners (IAOs) of the Organisation through effective networking structures, sharing of relevant experience, provision of training and creation of information risk reporting structures.

- Advise the Corporate Governance Group on the level of Information Risk Management performance within the Organisation, including potential cost reductions and process improvements arising etc.

Senior Directors and Heads of Service must:

- Ensure all new, current, and temporary\contract staff as well as Members are informed of their security responsibilities.

- Make sure that all users are trained to use correctly relevant computer systems/media.

- Ensure that only authorised users are allowed to access any of the Council's computer systems or information stores using agreed processes and procedures.

- Determine which individuals are to be given access to specific information.

- Make sure that documentation for all critical job functions are always maintained to ensure continuity in the event of an individual being unavailable.

- .
  When implementing any new information system, digital or manual, seek advice from Information Governance with respect to security.

- Make sure that all employees are aware of their responsibilities regarding maintaining confidentiality of information. Where highly sensitive information is being processed the staff involved must sign confidentiality (non-disclosure) agreements as part of their contract of employment.

  Make sure that all employees co-operate with the maintenance of the Information Asset Register and the ICT Asset inventory.

Line managers are responsible, within their functions, for:

- Understanding the information assets and ICT services for which they are responsible and the applicable access control requirements.

- Authorising employees to use and access information and ensuring that this is used for approved purposes only.

- The education and awareness of their employees to use information assets and ICT services correctly.

- Ensuring all employees conform to and are working in a manner consistent with Corporate Information Security policies and guidance.

- Investigating any security issue that members of staff raise in connection with their work and reporting those incidents, where appropriate, to the Information Governance Unit.

- Making sure that all their staff have read, understood and agree to the ICT Acceptable Use policy.

- Investigating and reviewing any breaches of the policy as a consequence of incidents or audits within their management area.

- Control of inventories related to ICT services equipment. (E.g. Hardware, Software, users and licenses).

- Ensuring the ICT Starters and Leavers team is given sufficient notice of new users so that their network accounts can be created ready for when the user commences work.

- Ensuring the ICT Starters and Leavers team is notified immediately when staff leave or move internally to another post or a Member ceases to represent the County Council, so that access rights can be revoked or amended.

- Returning any ICT equipment to SICT if it is no longer required due to business change or as a consequence of staff leaving or moving elsewhere within the organisation. The assets must not be retained by the individual even if they remain in the employment of the council unless agreed with SICT.

All Members and employees (including those under contract, work experience and agency staff) are:

- Responsible for conforming to the Corporate Information Security policies and guidance documents.

- Required to inform the ICT Service Desk on (01785) 278000 of any possible or suspected security incidents.

- Required to abide by the terms of the Data Protection Act 1998, Computer Misuse Act 1990 and any other relevant legislations / standards.

- Required to raise areas of concern regarding information security. In the case of Members, the Head of Member Services must be informed. Employees must inform their Line Manager. An alternative is to send a message to the confidential email address: ictsecurity@staffordshire.gov.uk

4. Organisation of Information Security

4.1 Information Security Infrastructure

Objective: To manage Information Security within the organisation.

4.1.1 The Audit and Standards Committee

The Committee is the appropriate member body to receive the Annual Information Governance Statement which includes a statement on ICT Security.

4.1.2 The Corporate Governance Group

The group has an oversight of all governance matters within SCC which includes the use of ICT and systems.

4.1.3 The Director of Strategy, Governance and Change

The director is the Monitoring Officer for SCC and is ultimately responsible for legal regulatory compliance across the organisation.

4.1.4 The Head of ICT

The Head of ICT has ultimate responsibility for ICT provision and systems across SCC and partners.

4.1.5 The Head of Information Governance

The Head of Information Governance is accountable for approving SCC security policies and practices to ensure a standard, comprehensive and industry best practice approach to security across all IT networks, PC's and applications systems

4.1.6 The Information Governance Team

The team has the overall responsibility for all security matters. It is responsible for ensuring there is a clear drive to achieve best practice in information security.

The Team will be responsible for:

- Reviewing and maintaining Information Security policies and guidance.
- Reporting on information security within the Council.

- Evaluating security technology, processes and the implementation of appropriate levels of security control.

- Ensuring compliance with relevant legislation.

- Making sure the Council's staff, partners, members and contractors\contracted suppliers are aware of their responsibilities and accountability for information security.

- Assessing the adequacy of specific information security controls for new or changed systems/services.

- Undertaking investigations into breaches of security policies

- Providing an advisory service on Information Security.

4.1.7 Staffordshire ICT (SICT)

SICT is responsible for:

- Reviewing controls and integrity procedures to make sure that they will not be compromised by changes to the technical infrastructure or underpinning processes.

- Identifying all computer hardware, software, systems, information and database entities on the Corporate Network that require amendment.

- Obtaining formal approval for changes before work commences.

- Ensuring that implementation is carried out to minimize business disruption.

- Ensuring that the system documentation is updated after any changes and that old documentation is archived or disposed of.

- Maintaining software standards for Corporate (excludes Business specific) software.

- Maintaining an audit trail of all change requests.

- Ensuring that operating documentation and user procedures are changed as necessary so that they are appropriate.

- Ensuring that changes being implemented take place at the right time and does not disturb business as usual.

4.2 Security of Third Party Access

Objective: To maintain the security of the County Council's information processing facilities and any information assets which are accessed by third parties.

All third party access must be requested through the Information Security Team in accordance with the providing Third Party Access Policy located here. It must be strictly controlled and monitored and a risk assessment process in line with the Third Party Access Policy, located here, must be followed. To adequately manage third party arrangements, managers within each directorate must make sure agreements are in place with any supplier/third party user requiring access to the Council's systems.

The agreement must require the third party to sign the Third Party Acceptance declaration that they will comply with the Council's security policies.

4.3 External Providers

Objective: To maintain security of information when the responsibility for information processing is provided by an external organisation.

External arrangements; both in relation to business process outsourcing and external information\system hosting must consider and address the risks, security controls and procedures (such as but not exhaustive) for information security, the integrity of information systems, personnel, data management, access and technical environment and provide for inspection of their environment in the contract between the parties.

5. Asset Classification and Control

5.1 Asset Management

Objective: To ensure that all significant assets are identified, responsibility is correctly determined and the right levels of protection are provided according to the importance and value of assets.

An organisation needs to be able to identify its assets and the relative value and importance of these assets. An inventory must be drawn up of all assets associated with Staffordshire County Council and then maintained accordingly. For the purpose of this policy, the term 'assets' includes:

a) **Information assets:** databases and data files, hard copy documents, system documentation, user manuals, training material, operational or support procedures, continuity plans, fallback arrangements;

b) **Software assets**: application software, system software, development tools and utilities;

c) **Physical assets:** computer and data communications equipment, magnetic media other supporting technical equipment (computer power supplies, air-conditioning units in Information Processing Suites),

SICT is responsible for

- Producing and maintaining a register of hardware and software assets purchased through SICT or visible on the Corporate Network

- Ensuring all software has relevant licences where it has been purchased by SICT.

Managers within each directorate are responsible for drawing up an inventory of all other assets associated with each information system owned by them. Each asset must be clearly identified together with its nominated owner, current location, asset value and description. The nominated ICT asset owner is responsible for the protection of that asset according to its classification. Managers will work with SICT on the maintenance of the ICT asset inventory and will notify SICT immediately when there are changes to the accuracy of the inventory (e.g., user changes, equipment moves, redundancy of systems or Information).
Managers will also work with Information Governance to contribute to the maintenance and accuracy of the Information Asset Register.

5.2 Information Security Classification

Objective: To ensure that information assets are appropriately classified so that they receive the right level of protection.

Information needs to be classified to indicate the need, priorities and degree of protection. The authority has implemented a Protective Marking Scheme which is located here.

The Protective Marking Scheme:

- Provides an appropriate set of protection levels for the Council's information and communicates the need for special handling procedures;
- Labels information according to how critical it is the Council, e.g. in terms of its required levels of integrity and availability;
- Allows for the fact that the classification level of any item of information may change over time;
- Outlines who is responsible for classifying an item of information and also the period after when classification must be reviewed.

Users must put the appropriate level of confidentiality on documents. All requests for information must be dealt with in accordance with the Data Protection Act (1998), the Freedom of Information Act (2000) and any other relevant legislation.

6. Personnel Security

6.1 Security in job definition and employment

Objective: To reduce the risks of human error, theft, fraud or misuse of facilities.

SICT will maintain a directory of authorised user accounts defining permissions and access rights to use Staffordshire ICT services. Temporary and external user accounts will be set to expire at the end of the contract period.

6.1.1 User Responsibilities

All users including those who are temporary and external must adhere to all Staffordshire County Council ICT policies including:

- ICT Acceptable Use Policy
- Clear Desk and Screen policy
- Third Party Access Policy
- Password Policy

Security policies will be continually reviewed and updated and it is the responsibility of all users to ensure they understand the policies which can be accessed here:

It is the responsibility of all users to comply with all Staffordshire County Council ICT policies.

Staffordshire County Council disciplinary procedures will be pursued where serious or intentional breach of policy is established.

6.1.2 Job Definitions

Employees with substantial Information Security responsibilities must have them detailed in their job descriptions.

Verification and screening checks appropriate to the role must be carried out at the time of job application. The County Council's Code of Conduct must be brought to the attention of all new employees.

6.2 User Security Awareness Training

Objective: To ensure that all users are fully aware of, and trained in all aspects of information security.

All users must receive training at the earliest date in the use of ICT facilities. All users as part of the induction process must receive training on the County Council's security policies and all other aspects of information security relevant to their directorate. All users have a personal responsibility to make themselves aware of the content of the corporate security policies and to adhere to these policies. If users are found to have breached these policies may be subject to appropriate disciplinary action.

6.3 Reporting Security Incidents

Objective: To minimise damage from security incidents and malfunctions, and to monitor and learn from such incidents.

Managers must ensure that users know the correct procedures for reporting potential security incidents.

Users must report potential breaches of ICT security immediately to the ICT Service Desk on 01785 278000 or if appropriate to their Line Manager. If they do not feel that they can report the issue to their Line manager or if the issue is of a sensitive or confidential nature then they can contact the Information Security team on the confidential email address: ictsecurity@staffordshire.gov.uk

An information security incident is any situation where confidential, sensitive or personal data is either lost (lost/stolen laptop, misplaced USB device) or misdirected (for example health information sent to wrong person/wrong address) – this may be either by physical mail or through electronic means. Guidance of what to do if there is a suspected Information Security incident can be found here.

7. Physical and Environmental Security

7.1 Secure Areas

Objective: To prevent unauthorised access, damage to and interference with business premises and information.

A list of secure areas must be maintained by SICT to protect rooms that contain servers, data communications, telephone equipment, and closets containing routers as well as switches and cabling.

Secure areas must be protected by appropriate entry controls to ensure that only authorised personnel are allowed access. Access to secure areas will be authenticated and validated. Visitors to secure areas must be supervised or cleared and their date and time of entry and departure recorded.

Where services have been contracted out to 3rd party suppliers then appropriate controls must be defined to ensure that equivalent controls are in place and are auditable.

7.2 Equipment Security

Objective: To prevent loss, damage or compromise of assets and interruption to business activities.

Equipment must be physically protected from security threats and environmental hazards and must be in line with appropriate good practice guidelines including the following:

- Physical security and access control.
- Fire detection and extinguishing systems.
- Temperature and humidity control.
- Dust free environment.
- Low risk from water damage.
- Surge free and stable uninterruptible power supply (UPS).
- Maintenance agreement, in line with manufacturer’s specifications.

8. Communications and Operations Management.

8.1 Server Security Standards

Objective: To establish standards for the base configuration of server equipment.

All the County Council's owned servers are the responsibility of the Infrastructure Manager who is responsible for the following:

- Base-lining servers to the Council's corporate standard e.g. Operating System and Database versions and build standards).
- Continually updating servers to make sure that they have the latest security updates and patches.
- Ensure the Patching Policy is adhered to.
- Maintaining the server as an asset.
- Creating and maintaining server configuration documents.
- Periodically subjecting servers to penetration tests so that they can be analysed for vulnerabilities.

Where any of services are to be provided by a third party supplier assurances must be sought from the supplier that the standards above will be incorporated as a minimum.

8.2 Operational Procedures and Planning

Objective: To ensure the correct and secure operation of information processing facilities

All information systems must have their operating procedures documented including start-up and close-down procedures, back-up, and equipment maintenance.

Wherever practical the following operations and applications change control procedures must be considered. These are:

- Identifying and recording significant changes.
- Assessing the potential impact of such changes.
- Formally approving procedures for proposed changes.
- Communicating change details to relevant people.
- Making sure procedures are in place identifying responsibilities for aborting and recovering from unsuccessful changes.

An appropriate incident management procedure must be used to ensure a quick, effective and orderly response to security incidents.

There must be a level of separation between development and test activities. To avoid unauthorised modification and access to operational software and data the following controls must be considered:

- Development and operational software must, where possible, run on different computer processors, or in different domains or directories.
- Development and testing activities must be separated as far as possible.
- Compilers, editors and other system utilities must not be accessible from operational systems when not required.
- Different log-on procedures must be used for operational and test systems, to reduce the risk of error. Users must be encouraged to use different passwords for these systems, and menus must display appropriate identification messages.
- Development users must only have access to operational passwords where controls are in place for issuing passwords for support of operational systems. Controls must ensure that these passwords are changed after use.

8.3 System Planning and Acceptance

Objective: To minimise the risk of system failures and maintain availability

Capacity demands need to be regularly monitored and projections made of future capacity requirements to ensure adequate processing power and storage are available to maintain the required system performance.

The operational requirements of new systems must be established, documented, and tested prior to their acceptance and use.

8.4 End User Computing Applications

Objective: To maintain the availability of local IT applications

The definition of an end user application is an in-house development using software such as spreadsheets or databases for the purpose of making service specific decisions. It could also include commercially purchased software used for a specific local purpose. Therefore end user applications do not include corporate software, operating systems or applications developed by Stafford ICT.

End user computing applications are local IT applications used for decision making. Therefore consideration must be made for their security and business continuity. For example the implications of loss of knowledge and management due to staff changes must be taken into account.
The owner of an end user computing application is the individual responsible for the outputs/outcomes of the system. The owner is responsible for the following:

- To ensure full documentation for the operation and maintenance of the application exists
- Provision is made for the back up of the application and related data

Formulae, standard calculations or data analysis elements of the software are periodically reviewed to ensure any legal, regulatory or business requirements are met

8.5 Protection against Malicious Software

Objective: To protect the integrity of software and information

The following detection and prevention controls must be put in place to protect against malicious software. These must be combined with user awareness:

- All Server, workstations, portable devices (e.g. handheld and laptops) will have up-to-date anti-virus software installed.

- All e-mail routed internally and externally will be filtered for potential

- Firewalls will be installed to control and monitor network traffic.

- Software installed must be compliant with software licenses and the installation of unauthorised software is prohibited this also includes plug-ins and screensavers.

- Anti-virus updates are automatically downloaded to equipment connected to the network. Remote users must connect to the network at least every 2 weeks as best practise but not exceed 4 weeks to download the latest anti-virus updates. Any failed anti-virus updates must be immediately reported to the ICT Service Desk.

- Users must not disable the anti-virus software.

8.5 Housekeeping

Objective: To maintain the integrity and availability of information processing and communication services.

Electronic Information Security involves protecting data from loss and corruption. Backup media must be housed in a secure area (see 7.1) and a copy also held securely off the premises in case of fire or water damage and must be in accordance with risk assessments.

Backup copies of essential business information and software must be taken daily.
Backup media must be retained and disposed in accordance with the County Council's retention schedules, the Data Protection Act (1998), and the Freedom of Information Act (2000)

8.6 Network Management

Objective: To safeguard information contained in the Council network and protect the supporting infrastructure.

Controls must be put in place to ensure the security of data in networks and the protection of connected and wireless services from unauthorised access. Responsibilities and procedures for the management of remote equipment, including equipment in user areas, must be established.

Only approved network connections must be used. Additionally, there must not be any use of unauthorised modems or wireless connections. Any network access point that is not in use must be de-activated. Wireless access must be in accordance with the Wireless Model.

Documents detailing the network infrastructure must be kept and maintained.

8.7 Media handling and security

Objective: To prevent damage to assets and interruptions to business activities, media must be controlled and physically protected.

Procedures must be in place to protect documents, computer media (tapes, disks, cassettes), input/output data and system documentation from damage, theft and unauthorised access.
All mobile devices including laptops and USB Memory sticks must be encrypted. Laptops must be connected to the network every 2 weeks, as best practice, but not exceed 4 weeks to ensure the latest security updates are applied.

Procedures must be drawn up for handling information consistent with its classification including:

- system documentation
- documents
- computing systems
- networks
- mobile computing
- mobile communications
- mail
- voice mail
- voice communications

8.8 Exchanges of information and software

Objective: To prevent loss, modification or misuse of information exchanged between organisations.

Exchanges of information and software between organisations must be controlled, and must be compliant with relevant legislation.

Controls must be applied to protect electronic mail and on-line transactions across open networks such as the internet to protect against fraudulent activities, contract dispute and disclosure or modification of information.

Electronic mail is a high-risk service and its use is governed by the County Council ICT Acceptable Use Policy.

All users with access to e-mail facilities must be trained in the ICT Acceptable Use Policy and must sign a declaration form stating that they understand the policy and agree to abide by its contents.

Controls must be put in place to protect the integrity of electronically published information to prevent unauthorized modification which could harm the reputation of the publishing organization. This will involve a formal authorisation process before information is made publicly available.

For guidance on the current secure mechanisms available to exchange information contact SICT.

9. Access Control

9.1 User Access Management

Objective: To prevent unauthorised access to information systems

Users must follow good security practices in the selection and use of passwords in accordance with the County Council's Password Policy.

Procedures must be used to ensure the ICT Starters and Leavers team are made aware when users leave or are transferred to another department, or when Members cease to represent the council, and they will be responsible for the prompt removable or amendment of network accounts.

User's access rights must be appropriate to their responsibilities and they must be periodically reviewed to ensure that they are still relevant.

Privileged Access to the corporate network or ICT systems must only be granted in accordance with the Privileged Access Policy located here.

Emergency arrangements must be made to deal with occasions where a privileged person is not available. A user ID and password must be held with strict procedures for emergency issue. Should the emergency procedure be used it must be reviewed by the Server Support Manager and the emergency user ID and password changed.

9.2 Network Access Control

Objective: Protection of networked services

Access to both internal and external networked services must be controlled and users must not be allowed to access areas of the network that are not relevant to their responsibilities.

Wireless network connections must be configured in strict accordance with SCC corporate standards as specified in the Wireless Policy.

9.3 Application access control

Objective: To prevent unauthorised access to information held in information systems.

Security facilities must be used to restrict access within application systems. Logical access to software and information must be restricted to authorised users. Measures need to be defined for users to access business information and application systems including the security of other systems in which information resources are shared.

9.4 Monitoring system access and use

Objective: To detect unauthorised activities.

Security relevant event logs must be kept which will assist in monitoring the network for unauthorised access. Event logs will be reviewed regularly by the Information Security team. The logs must include the following:

- User name.
- Date and time for log-on and log-off.
- Computer name.
- Records of successful and rejected system access attempts

9.5 Mobile Computing and Remote Working

Objective: To ensure information security when using mobile computing and remote working facilities.

Users must only be allowed to use mobile computing facilities once they have received training from SICT and have signed the Mobile Device and Removable Media Guidance and ICT Acceptable Use Policy.

Users must connect their laptops to the corporate network at least a minimum of once a month. This will ensure virus protection software is up-to-date and any patches are installed.

9.5.1 Wireless Technology

Wireless connections must only be installed following authorisation and in strict accordance with the County Council's Wireless Guidance.

9.5.2 Ad Hoc Networks

If other wireless connectivity is required then a secure connection using appropriate encryption must be established to secure communication with other devices. For further guidance contact SICT.

10 System Development and Maintenance

10.1 Security requirements of systems

Objective: To ensure that security is built into information systems.

Security requirements must be identified and agreed prior to the development of any information systems. Where relevant risk assessments of proposals will be carried out by the Information Security team

10.2 Cryptographic Controls\Encryption

Objective: To protect the confidentiality, authenticity or integrity of information.

Consideration must be given to the regulations and national restrictions of cryptographic policy. Products must be selected that provide the required protection with a secure system of key management.

Encryption must be applied to protect the confidentiality of Confidential and Restricted data. The Protective Marking Scheme provides further guidance.

Staffordshire ICT will by default encrypt all Mobile devices connecting to the corporate network including Laptops and USB sticks.

Encryption facilities are available and must be used for the transmission of data to non-council recipients in line with the Protective Marking Scheme, unless an alternative has been approved by a SIRO

10.3 Security of systems files

Objective: To ensure that ICT projects and support activities are conducted in a secure manner. Access to system files must be controlled.

Physical or logical access must only be given to suppliers for support purposes when necessary, and with management approval. The supplier's activities must be monitored.

Test data must be fictitious or de-personalised to avoid breaches of

Strict control and documentation must be maintained by SICT over access to program source libraries on servers as they provide a starting point for unauthorised modification of a system.

10.4 Security in development and support processes

Objective: To maintain the security of application system software and information

When designing and developing a new application system or modifying an existing one, security requirements must include an appropriate control and audit trail or action plans of security procedures to minimise the risk of data integrity.

Formal control and co-ordination of all changes must be implemented using project management standards with appropriate authorisation for each change at all stages of development.

11 Business Continuity Management

11.1 Aspects of business continuity management

Objective: To counteract interruptions to business activities and to protect critical business processes from the effects of major failures or disasters.

11.1.1 Business continuity and impact analysis

Business Continuity plans are the responsibility of Business Managers and must consider the criticality of information and ICT systems as an element of the overall plan.

ICT Disaster Recovery will underpin Business Continuity and is the responsibility of SICT using agreed Business priorities and criticalities to determine a restoration routine in the event of a catastrophe.

Disaster Recovery (DR) plans and procedures must be in place for all mission critical systems used throughout the authority, in the event of interruptions to business activities.

Critical business activities must be identified, by Business Managers and the underpinning ICT systems should be identified to SICT. SICT will then carry out risk assessments to determine the possible cause of interruptions and their impact on both ICT and business processes. The risk assessment must include an estimate of the full recovery costs, (ICT and non-ICT) in order for financial arrangements to be included in contingency planning.

The responsibility of SICT does not extend to externally hosted services or systems the responsibilities for such services need to be agreed between the commissioner of the service and the supplier and defined in the associated contract.

11.1.2 Backup and Recovery requirements

All data must be backed up at regular periods and this must be the responsibility of individuals as well as the Technical Services teams. This will ensure that important information can be recovered in the event that data is lost due to hardware, software or human error.

11.1.3 Testing of Backup and Recovery Plans

Business continuity recovery plans must be tested regularly, plans re-assessed and maintained to ensure successful recovery in the event of a failure.

12 Compliance

12.1 Compliance with legal requirements

Objective: To avoid breaches of any criminal and civil law, statutory, regulatory or contractual.

The Council's policies are compliant with and are reviewed to ensure continuing compliance with relevant legislation including the following Acts and any revisions to said Acts:

Data Protection Act (1998),

The Copyright, Designs and Patents Act 1988

Computer Misuse Act (1990)

Regulation of Investigatory Powers Act 2000

Human Rights Act 1998

Freedom of Information Act (2000).

Appendix A

Glossary of Terms

Antivirus Software: Antivirus software is an application that searches your hard drive and any other removable drives for any known or potential viruses.

Bluetooth: Bluetooth wireless technology makes it possible to transmit radio signals, over short distances, between computers and other devices, thereby simplifying communication and synchronisation between devices. Bluetooth eliminates the need for wires and cables between both stationary and mobile devices, it facilitates both data and voice communication.

Business Continuity (BC): The strategic and tactical capability of the organisation to plan for and respond to incidents and business disruptions in order to continue business operations at an acceptable predefined level.

Cryptographic Control: Is a range of methods which can be implemented to protect the confidentiality, authenticity or integrity of information.

Disaster Recovery (DR): The process, policies and procedures for the recovery or continuation of technology infrastructure in the event of a disaster. Disaster Recovery is a component of Business Continuity.

Encryption: Is the alteration of data into a form, called cipher text that cannot be easily understood by unauthorised persons. **Decryption** is the process of converting encrypted data back into its original form, so it can be understood.

Firewall: Firewall Software is a basic requirement for any organisation to prevent hacking, virus, and other security risks. Firewall software is designed to prevent unauthorised access to a computer or network that is connected to the Internet.

ICT Service Desk: Staffordshire County Council ICT support helpline desk, 01785 278000

Patch: A patch (sometimes called a "fix") is an update or a repair for a piece of programming. A patch is the immediate solution that is provided to users by the software manufacturer. Patches are supplied by the software manufacturers.

Penetration Tests: The process of performing a penetration test is to make sure that new and existing applications, networks and systems are not vulnerable to a security risk that could allow unauthorised access to resources.

Remote Users: Users who access Staffordshire County Council applications and resources through dialup or broadband connections.

PIN: Personal Identification Number.

SICT: Staffordshire Information Communication Technology. This includes the following support teams: Communications, Desktop Support, Network Infrastructure and Server Support.

The Council: Staffordshire County Council.

Two Factor Authentication (2FA): Is a two-step process for accessing a computer network or system. The two steps usually refer to something you know and something you have. For example a token is something you have and a password is something you know.

Universal Serial Bus (USB): Is a standard form of connection for a wide range of devices including printers, keyboards smart phones, cameras etc.

Wi-Fi: A technology that allows a device to connect to the internet or network wirelessly using radio waves.