Policy Document

PO 01

Information Security

August 2017
Para 7 insert Officers of the County Council are required to comply with this policy/procedure in respect of its provisions and ethos. Failure to do so may be regarded as a breach of the Officers’ Code of Conduct and could result in action being taken against the member of staff concerned.’

Section 5 insert Civil Contingencies Act 2004 into identified risk list and compliance

Review by SMT – No changes identified

Review after PWC audit

Review due to directorate change and annual review. Change of name from T&C Services to Technology and Change

Change to incorporate PSN and titles

Changes to ISO 27001 standard from 2005 standard to 2013 standard. Incorporation of new controls included within new standard. Changes of organisational structure and all names removed and replaced with job titles

Change from ICT/IT to T&C

Review by T&C Leadership Team

Annual review. Removal of old revision history

This document requires the following approvals:

<table>
<thead>
<tr>
<th>Sponsor Approval</th>
<th>Name</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Senior Information Risk Officer</td>
<td></td>
<td>May 2013</td>
</tr>
<tr>
<td>Assistant Director of Technology and Change</td>
<td></td>
<td>May 2013</td>
</tr>
<tr>
<td>Audit and Information Assurance Manager</td>
<td></td>
<td>May 2013</td>
</tr>
</tbody>
</table>

This document will be distributed to:

<table>
<thead>
<tr>
<th>Name</th>
<th>Job Title</th>
<th>Email Address</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Contents

1. Policy Statement 5
2. Purpose 5
3. Scope 5
4. Definition 5
5. Risk 6
6. Applying the policy 6
6.1 Management of security 6
6.2 Information security awareness training 7
6.3 Contracts of employment 7
6.4 Security control of assets 7
6.5 Access controls 7
6.6 User access controls 7
6.7 Computer access controls 7
6.8 Application access control 7
6.9 Equipment security 8
6.10 Computer and Network procedures 8
6.11 Information Risk assessments 8
6.12 Information security incidents and weaknesses 8
6.13 Classification of sensitive information 8
6.14 Protection from malicious software 8
6.15 User media 8
6.16 Monitoring system access and use 9
6.17 Accreditation of information systems 9
6.18 System change controls 9
6.19 Intellectual property rights 9
6.20 Business continuity and disaster recovery plans 9
7. Policy Compliance 9
8. Policy Governance 10
9. Review and Revision 10
10. References 10
11. Key Messages 11
1. **Policy Statement**

This top level information security policy is a key component of North Yorkshire County Council overall information security management framework and must be considered alongside more detailed information security documentation including system level security policies, security guidance and protocols or procedures. The policy should be read in conjunction with other policies listed in Section 10.

The aim of information security is to protect the council’s information assets from a wide range of threats whether internal or external, deliberate or accidental, in order to ensure business continuity and minimise the impact of adverse events on customers and staff.

2. **Purpose**

The objectives of this Policy are to preserve:

- **Confidentiality** - Access to Data shall be confined to those with appropriate authority.
- **Integrity** – Information shall be complete and accurate. All systems, assets and networks shall operate correctly, according to specifications.
- **Availability** - Information shall be available and delivered to the right person, at the time when it is needed and in the relevant format.

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

- Ensuring that all employees and members are aware of and fully comply with the relevant legislation. As described in this and other policies.
- Describing the principals of security and explaining how they shall be implemented in the council.
- Information includes data printed out or written on paper, stored on computers, transmitted across networks, sent by fax, stored on tapes and disks or spoken in conversation and over the telephone.
- To introduce a consistent approach to security ensuring that all employees and members fully understand their responsibilities.
- Creating and maintaining within the organisation 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.

In delivering its services the council will process payments electronically and has to be compliant with PCI DSS standards. This is a set of security standards that apply across the card payment industry worldwide that help safeguard cardholder information and improve consumer confidence. The standard includes requirements for security management, policies, procedures, and network architecture and software design. This comprehensive standard is intended to pro-actively protect customer account data.

There are six goals of PCI compliance security standards:

1. Building and maintaining a secure network
2. Protecting cardholder data
3. Maintaining a vulnerability management program
4. Implementing strong access control measures
5. Regular monitoring and testing of networks
6. Maintaining an information security policy

These controls are included and maintained within the councils certified ISMS, all employees that deal with online payments should make themselves aware of the policies contained within the ISMS.
3. **Scope**

This policy applies to all information, information systems, networks, applications and locations in North Yorkshire County Council

Ultimate responsibility for information security rests with the Senior Information Risk Officer of the council, but on a day-to-day basis the Senior Information Security Compliance Officer and the Data Protection Officer shall be responsible for managing and implementing the policy and related procedures and associated policies.

4. **Definitions**

**Information System (IS)**

An Information System is defined as a system that requires the use of and the support of the council’s IT infrastructure and/or a system that stores or manipulates data and/or any system that requires ongoing support from Technology and Change

**System Owner (SO)**

The System Owner (SO) is the individual who has overall responsibility for an information system, its governance and usage.

**System Administrator (SA)**

The System Administrator (SA) is responsible for the day to day maintenance of the system. This is separated from the system owner role however both roles may be done by the same person.

**System User (SU)**

Individuals who access and use the information system to perform tasks defined within their access roles and privileges.

5. **Risks**

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 customers.

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

- The Data Protection Act (1998)
- The Data Protection (Processing of Sensitive Personal Data) Order 2000.
- The Computer Misuse Act (1990)
- The Health and Safety at Work Act (1974)
- Freedom of Information Act 2000
- Health & Social Care Act 2001
- Health & Social Care Act 2008
- Mental Health Act 1983
- Mental Health Act 2007
- Disability Discrimination Act (DDA) 1995
6 Applying the Policy

6.1 Management of Security

The Senior Information Security Compliance Officer shall be responsible for implementing, monitoring, documenting and communicating security requirements for the council.

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 shall comply with information security procedures including the maintenance of data confidentiality and data integrity.

The Information Security Policy shall be maintained, reviewed and updated by the Corporate Information Governance Group. This review shall take place annually and be recorded within the revision history of the policy.

Line managers shall be individually responsible for the security of their physical environments where information is processed or stored.

Each member of staff shall be responsible for the operational security of the information systems they use.

Each system user shall comply with the security requirements that are currently in force and identified within the system specific policy, and shall 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 shall be in operation before access is allowed. These contracts shall ensure that the staff or sub-contractors of the external organisation shall comply with all appropriate security policies.

6.2 Information Security Awareness Training

Information security awareness is included in the staff induction process. ELearning covering Information Security, Data Protection and Freedom of Information is mandatory for all NYCC staff.

An ongoing awareness program has been established in order to ensure that staff awareness is refreshed and updated as necessary. Online training is available to all staff.

6.3 Contracts of Employment

Staff security requirements shall be addressed at the recruitment stage.

6.4 Security Control of Assets

Each T&C asset, (hardware, software, application or data) shall have a named custodian who shall be responsible for the information security of that asset.

6.5 Access Controls
Only authorised personnel who have a justified and approved business need shall be given access to restricted areas containing information systems or stored data.

### 6.6 User Access Controls

Access to information shall be restricted to authorised users who have a bona-fide business need to access the information.

### 6.7 Computer Access Control

Access to computer facilities shall be restricted to authorised users who have a business need to use the facilities.

### 6.8 Application Access Control

Access to data, system utilities and program source libraries shall be controlled and restricted to those authorised users who have a legitimate business need. Authorisation to use an application shall depend on the availability or procurement of a license from the supplier.

### 6.9 Equipment Security

In order to minimise loss of, or damage to, all assets, equipment shall be physically protected from threats and environmental hazards.

### 6.10 Computer and Network Procedures

Technology and Change are responsible for ensuring management of computers and networks are controlled through standard documented procedures that have been authorised.

### 6.11 Information Risk Assessment

The core principle of risk assessment and management requires the identification and quantification of information security risks in terms of their perceived value of asset, severity of impact and the likelihood of occurrence.

Once identified, information security risks shall be managed on a formal basis by Technology and Change. They shall be recorded within a baseline risk register and action plans shall be put in place to effectively manage those risks. The risk register and all associated actions shall be reviewed at regular intervals. Any implemented information security arrangements shall also be a regularly reviewed feature of the council's risk management program. These reviews shall help identify areas of continuing best practice and possible weakness, as well as potential risks that may have arisen since the last review was completed.

### 6.12 Information security incidents and weaknesses

All information security events and suspected weaknesses are to be reported to the Senior Information Security Compliance Officer. All information security events shall be investigated to establish their cause and impacts with a view to avoiding similar events.

### 6.13 Classification of Sensitive Information

A consistent system for the classification of information within Government organisations enables common assurances in information partnerships, consistency in handling and retention practice when information is shared with non-government bodies.

The council shall implement appropriate information classifications controls, based upon the results of formal risk assessment and guidance contained within the Information Governance Toolkit to secure their information assets.
The Senior Information Security Compliance Officer or Data Protection Officer should be contacted for further guidance and instruction.

6.14 Protection from Malicious Software

The council shall use software countermeasures and management procedures to protect itself against the threat of malicious software. All staff shall be expected to co-operate fully with this policy. Users shall not install software on the council's property without permission from Technology and Change.

6.15 User media

Removable media of all types that contain software or data from external sources, or that have been used on external equipment, require the approval of Technology and Change before they may be used on council systems. Such media must also be fully virus checked before being used on the council's equipment.

6.16 Monitoring System Access and Usage

An audit trail and log will be kept of all monitoring that is undertaken

The council has in place routines to regularly audit compliance with this and other policies. In addition it reserves the right to monitor activity where it suspects that there has been a breach of policy. The Regulation of Investigatory Powers Act (2000) permits monitoring and recording of employees' electronic communications (including telephone communications) for the following reasons

- Establishing the existence of facts
- Investigating or detecting unauthorised use of the system
- Preventing or detecting crime
- Ascertaining or demonstrating standards which are achieved or ought to be achieved by persons using the system (quality control and training)
- In the interests of national security
- Ascertaining compliance with regulatory or self-regulatory practices or procedures
- Ensuring the effective operation of council systems

Any monitoring will be undertaken in accordance with the above act and the Human Rights Act (1998)

6.17 Accreditation of Information Systems

The council shall ensure that all new information systems, applications and networks include a security plan and are approved by Technology and Change before they commence operation.

All system owners should develop a system specific policy prior to any system going live in order to distinguish between the security management considerations and requirements of the system. Specific responsibilities must be assigned and obligations communicated directly to those who use the system.

6.18 System Change Control

Changes to information systems, applications or networks shall be reviewed in line with the change control policy. Technology and Change must be involved in this process.

6.19 Intellectual Property Rights

The council shall ensure that all information products are properly licensed and approved by Technology and Change. It is the responsibility of system owners to work with Technology and Change to ensure this takes place.
Users shall not install software on the council’s property without permission from Technology and Change.

6.20 Business Continuity and Disaster Recovery Plans

The council shall ensure that business impact assessment, business continuity and disaster recovery plans are produced for all mission critical information, applications, systems and networks. Regular backups of essential business information must be taken to ensure that the Council can recover from a disaster, media failure or error. Full back up documentation, including a complete record of what has been backed up along with the recovery procedure, must be stored at an offsite location in addition to the copy at the main site and be readily accessible.

7. Policy Compliance

Officers of the County Council are required to comply with this policy in respect of its provisions and ethos. Failure to do so may be regarded as a breach of the Officers’ Code of Conduct and could result in action being taken against the member of staff concerned.

If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).

If you do not understand the implications of this policy or how it may apply to you, seek advice from the Senior Information Security Compliance Officer.

The Senior Information Security Compliance Officer shall keep the Corporate Information Governance Group and senior management informed of the information security status of the council by means of regular reports and presentations any serious security breaches will be reported to the Information Commissioners Office once approved by the Senior Information Risk Officer.

8. Policy Governance

The following table identifies who within the council is Accountable, Responsible, Informed or Consulted with regards to this policy. The following definitions apply:

- **Responsible** – the person(s) responsible for developing and implementing the policy.
- **Accountable** – the person who has ultimate accountability and authority for the policy.
- **Consulted** – the person(s) or groups to be consulted prior to final policy implementation or amendment.
- **Informed** – the person(s) or groups to be informed after policy implementation or amendment.

<table>
<thead>
<tr>
<th>Responsible</th>
<th>Senior Information Security Compliance Officer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accountable</td>
<td>Senior Information Risk Officer</td>
</tr>
<tr>
<td>Consulted</td>
<td>Audit and Information Assurance Manager, Corporate Information Governance Group</td>
</tr>
<tr>
<td>Informed</td>
<td>All Council Employees, All Temporary Staff, All Contractors and All Third-party Suppliers.</td>
</tr>
</tbody>
</table>

This policy shall be subject to audit by internal and external auditors.

9. Review and Revision

This policy will be reviewed as it is deemed appropriate, but no less frequently than every 12 months.
Policy review will be undertaken by the Senior Information Security Compliance Officer in consultation with the Corporate Information Governance Group.

10. **References**

The following council policy documents are directly relevant to this policy, and are referenced within this document:

- PSN (GCSx) Acceptable Usage Policy and Personal Commitment Statement.
- Software Policy.
- T&C Access Policy.
- Internet Usage Policy.
- Computer, Telephone and Desk Use Policy.
- Remote Working Policy.
- Portable Media and Encryption Policy.
- Information Security Incident Management Policy.
- Employee Guide to Information Security
- Email Policy
- T&C Asset Policy
- Use of T&C Equipment Policy
- Acceptable use Policy
- Incident Policy
- Mobile Working Policy
- Disaster Recovery Policy
- Business Continuity Policy
- Risk Assessment Policy
- Remote Access Policy
- Disposal/ Recycling Policy

The following legislation is pertinent to this policy

- The Data Protection Act (1998)
- The Data Protection (Processing of Sensitive Personal Data) Order 2000.
- The Computer Misuse Act (1990)
- The Health and Safety at Work Act (1974)
- Freedom of Information Act 2000
- Health & Social Care Act 2001
- Health & Social Care Act 2008
- Mental Health Act 1983
- Mental Health Act 2007
- Disability Discrimination Act (DDA) 1995
- Disability Discrimination Act (DDA) 2005
- Electronic Communications Act 2000
- Intellectual Property 1994

11. **Key messages**

- Users shall not install software on the council's property without permission from Technology and Change
- All information security events and suspected weaknesses are to be reported to the Information Security Officer.
- Each member of staff shall be responsible for the operational security of the information systems they use.
- Only authorised personnel who have a justified and approved business need shall be given access to restricted areas containing information systems or stored data.