Northumberland County Council

DOCUMENT REFERENCE	VERSION	DATE OF THIS VERSION	DATE OF ORIGIN
InformationSecurityand TransportationTransferand SharingofDataPolicy	v2.0	22/04/2016	

	APPROVED BY	APPROVAL DATE
1	Information Governance Group	12/08/2016
2	Digital Programme Board	01/07/2016

DATE REVIEWED	REVIEWED BY	APPROVAL DATE	NEXT REVIEW DATE

Amendment History

VERSION	DATE	DESCRIPTION
v1.0	30/07/2013	Final Version
v1.1	10/10/2013	Amendments 7. System access and Passwords to include revisions to password policy as mandated by PSNA and CESG guidance.
v1.2	02/10/2013	Moved document to new standard policy format. Added reference to the NCC Secure Workspace Policy (page 14)
v2.0	22/04/2016	Combined Information Security and Transportation Transfer and Sharing of Data Policy - Google Rollout

Information Security and Transportation, Transfer and Sharing of Data Policy

1. Scope

This Policy applies to all elected Members, employees, or any other person who has responsibility for, or is required to access or process data obtained and stored by or on behalf of Northumberland County Council (NCC).

The policy covers the storage, processing, transporting, sharing and disclosing of Council data, and the security controls required to maintain the confidentiality and integrity of the data.

The policy should be read in conjunction with the Mobile Computing Policy, Data Quality Policy, Internet and Email Usage Policy, Using Your Own Device Policy and the Data Protection Policy.

2 Purpose

The purpose of this policy is to describe the rules and procedures to assist in the protection of all information assets owned and used by NCC from the risks posed by inappropriate use and access.

Inappropriate use of information and information systems exposes NCC to unnecessary risks. Examples include virus attacks, compromise of network systems and services, unlawful disclosure of information, regulatory and legal issues.

It is important that you comply with this policy and you understand what is required from you.

3. Introduction

NCC encourages employees to use new technology to enhance business efficiency, performance and customer service, as well as assisting personal development.

This policy includes all types of hard copy information and “communications facilities” which includes telephones (mobile and desk), Internet, Intranet, e-mail, google accounts, applications, application data and supporting infrastructure.

The word “computer” refers to any device that can get direct or indirect access to corporate information such as a PDA, Smart Mobiles, Blackberry, PC, laptop, etc.

This policy is designed to help you understand our expectations in the use of these business resources and to minimise potential legal or other risks when you use these communications facilities at work or on a personal device for work purposes.

4. Definitions

4.1 Personal and sensitive data

4.1.1 In the context of this Policy, data means information in the Council's care. The information may be held or moved in a number of different ways, such as:

- Paper
- Floppy / hard disk
- Memory stick
- CD-Rom and DVD
- Email
- Over the telephone
- By video conference
- Photographs
- Microfilm
- Computer systems

4.1.2 Data can include information about the Council's customers as well as other kinds of information used in the running of the Council's business, such as management or personnel records, policy documents and staff instructions.

4.1.3 Very basic information about an individual, such as name, address, phone number etc. can be misused, and if it includes additional personal data such as date of birth, bank account details etc., the impact of such misuse will be greater.

4.1.4 A large collection of data contained in one place can constitute a greater risk than the individual items of data within it.

4.2 Data Quality

4.2.1 Data Quality can be defined as being the creation, processing and management of Council information in such a way as to ensure:

- Its authenticity
- Its reliability
- Its integrity
- Its usability

4.3 Data Protection

4.3.1 Data Protection refers to the principles and provisions of the Data Protection Act 1998, which seeks to govern the secure management of personal data, and in particular:

- The obtaining of personal data
- The storage and security of personal data
- The use of personal data
- The disposal and/or destruction of personal data
- The accuracy of personal data

For further information please refer to our Data Protection Policy

5. Risks and impact

5.1 There are a number of risks associated with the transportation, sharing and transfer of data, including but not limited to:

5.1.1 Information being lost, damaged or intercepted in transit, e.g. stolen/lost laptops or memory sticks, opened envelopes.

5.1.2 Delivery service delivering mail incorrectly

5.1.3 Information being sent to the wrong address or being intercepted when sent by email, post or fax.

5.1.4 Information received within the organisation but delivered to the wrong person.

5.1.5 Confidential conversations being overheard.

5.1.6 Personal information not being disposed of appropriately.

5.2 These and other risks have the potential to impact on:

5.2.1 The individuals whose information has been put at risk

5.2.2 Users whose actions placed the information at risk. Their actions may lead to disciplinary action, and there may also be legal implications.

5.2.3 The organisation itself may experience a lack of public trust and confidence, and there is potential for prosecution under information legislation.

6 Security Classification

Everyone who works within NCC has a duty to respect the confidentiality and integrity of any information and data that they access. This applies to all information that users collects, stores, processes, generates or shares to deliver services and conduct business, including information received from or exchanged with external partners.

Users also have a responsibility to safeguard any information or data that they access, irrespective of whether it is marked or not in accordance with the governments classification scheme.

The security classification of **OFFICIAL** covers the majority of information that is created or processed by the public sector. This includes routine business operations and services, some of which could have damaging consequences if lost, stolen or published in the media, but are not subject to a heightened threat profile.

The **OFFICIAL-SENSITIVE** classification should not be confused with a separate classification; it is a classification to denote **OFFICIAL** information that is of a particular sensitive nature but that can be managed on **OFFICIAL** systems and infrastructure.

Users must ensure that access to **sensitive** data must ONLY be granted on the basis of a genuine business need. The compromise, loss or misuse of sensitive information may have a significant impact on an individual and an organisation.

Google's **Gmail** handles information securely up to a classification of **Official Sensitive.** Gmail messages are encrypted between Gmail and the computer and are also encrypted as the messages travel around Google's data centers. As long you use strong passwords on secure machines and implement Google's two-factor authentication then Gmail is perfectly safe in most cases.

NCC information asset owners are responsible for identifying any sensitive information and for putting in place appropriate business processes to ensure that it is securely handled. They should also know whether or not the recipient of any data is sufficiently secure.

7. General rules

7.1 System Access and Passwords

It is a criminal offence under the Computer Misuse Act, 1990 to deliberately attempt to access a system to which you have no authority.

Information Services (IS) regularly monitor systems and unauthorised attempts at accessing systems may be investigated.

All computer users are given a Username and Password; these are unique and must not be shared with any other employee.

No user is permitted to log onto any other user's account - In the (unlikely) event that there is a requirement to access another user's account; this must be requested via Line Manager who will request the appropriate approval via the IS Service Desk.

Passwords should not be written down, or kept where others might find them.

Passwords should be hard to guess and contain at least ten characters. Passwords must include a mixture of upper and lower case, numbers and special characters such as: ! , #, £, $.

All users must ensure that they log out successfully from systems when they are finished using them.

Passwords should be changed at regular intervals. A number of Systems are configured to force password changes at regular intervals.

7.2 Disclosure

7.2.1 Disclosure of data by telephone / SMS

7.2.1.1 Data must never be given out over the phone or by any other verbal means unless it is absolutely clear who the data is being given to and that they are entitled to that data and are ready and able to accept it. Use of a security word should also be considered to validate information sharing where appropriate.

7.2.1.2 If using text (SMS) messages for personal information, the recipient's consent to be being contacted in this way must be obtained.

7.2.1.3 Coded messages must be considered, and all messages received or sent must be documented and deleted immediately.

7.2.1.4 A dedicated work phone must be used for SMS messaging, with named users responsible for its physical security and access password.

7.2.2 Disclosure of data by Fax

7.2.2.1 Sensitive information should not be sent via fax.

7.2.2.2 Confirmation that the fax machine is in a secure location is required.

7.2.2.3 If sending personal information by fax, pre-programmed speed-dialling must not be used, and top sheets must be clearly marked “Private and Confidential”, together with the number of pages being sent and the contact details of the sender.

7.2.2.4 A time must be agreed with the recipient for the sending of the fax, and confirmation of delivery or non-delivery must be given.

7.2.3 Disclosure of hard copy data by external and internal mail

7.2.3.1 Information transported by surface mail must be by recorded delivery and must be protected from unauthorised access and environmental damage. External organisations should be requested to use secure post when forwarding confidential information, using tamper-evident packaging when possible.

7.2.3.2 When using internal mail confidential information must be placed in clearly identifiable envelopes and must be protected from loss and accidental viewing, using lockable storage equipment where appropriate.

7.3 Unattended Equipment

Computer equipment that is logged on and left unattended can present a tempting target for unscrupulous users or third parties on the premises. Unauthorised access of unattended equipment can result in harmful or fraudulent use.

Equipment should therefore always be safeguarded appropriately – especially when left unattended.

IS has implemented controls to help assist the user. Devices must have a password protected screen-lock.

Users are required to screen-lock their computers prior to leaving them unattended.

7.4 Disclosure of IS Information

Employees should not disclose information relating to NCC's IS facilities to anyone outside NCC, without express permission. Any telephone or e-mail canvassing for information should be passed directly to IS.

7.5 File Storage on local device

All data saved to a mobile device must be transferred to a network drive as soon as possible. The data must then be removed from the device as soon as practicable in order to minimise the amount of personal / confidential or corporate information potentially available to anyone who may attempt to access the device.

When user uses a chrome device e.g. a chrome book and loses internet connection the device will automatically sync the data as soon as an internet connection is re-established.

However when the user uses a windows based PC or laptop using windows software (as opposed to Google Apps) and loses internet connection they must store any data required on the local windows device. When an internet connection is re-established the employee must ensure that they copy the data across from the local windows device to the required network destination.

8. Transfer and sharing of data to third parties

8.1. Personal data must not be downloaded to mobile devices or to USB sticks or emailed as an attachment or in the body of an email sent to an external address without secure protection such as encryption in accordance with the ICO's Data Sharing Code of Practise.

8.2 Employees must only send what is absolutely required to be sent.

8.3 Initial questions to consider:

8.3.1 Do you know what the data contains?
8.3.2 Are you sure you have the authority to send the data? If not, consult with line manager within the department or service
8.3.3 Does the data need to be sent at all?

8.4 It is recognised that there are circumstances under which a legitimate request may be received for copies of data held by the Council – an example may be a system support company requiring a copy of a database, or access to a database in order to carry out support or maintenance work.

8.5 Enabling of access to a database must always be considered preferable to the copying of the data to portable media such as laptops, CD or memory sticks.

8.6 If a request is received for access to or copies of a database which contains personal or sensitive corporate data, the appropriate senior officer must confirm that the access or copying is legitimate.

8.7 Consideration must be given to enabling secure connection to the network to enable the company or individual to access the data remotely.

8.7.1 The Network Manager must be consulted about setting up this process, and the Council's Code of Connection must be completed.

8.8 In both cases the company or individual must be made aware of the Council's Data Protection Policy in the case of personal data, and must be required to complete the Council's Confidentiality Agreement and comply with all of its requirements.

8.9 Only if on-site or remote network access is not possible should consideration be given to copying the data to a CD, DVD or other removable storage device or using cryptshare.

8.9.1 Copying must take place under secure and controlled circumstances, and only when authorised by an appropriate senior officer.

8.9.2 Only sufficient data must be copied for the purpose.

8.9.3 The removable device must be password protected in an appropriate manner.

8.9.4 If a CD, DVD or other removable storage device is to be sent to the company or individual, this must be by Recorded Delivery.

8.9.4.1 The name and address of the recipient must be entered clearly on the envelope or parcel, which must be marked "Private and Confidential" and be securely packaged to prevent loss or damage during transit.

8.9.5 The data must not be supplied until the company or individual has been made aware of the Council's Data Protection Policy in the case of personal data, and has completed the Council's Confidentiality Agreement and agreed to comply with all of its requirements.

9 General rules for visitors to Council premises

9.1 Users must ensure that visitors are aware of this aspect of this policy:

9.1.1 Visitors must not connect any mobile device, or attach any media to any equipment belonging to the Council without prior authorisation, which must be from a relevant Manager.

9.1.2. Any approved connection must take place under appropriate supervision.

9.1.3 Visitors must not under any circumstances copy Council information of any description to any device or media without explicit consent. This may be regarded as theft of Council property and result in legal action.

9.1.4 Where possible, visitors must use “stand-alone” PCs or laptops for such devices or media instead of networked equipment

10 Physical Security Controls

Only members of IS (or IS approved contractors) are permitted to move any non-portable IT equipment, whether within an office or to another site.

No peripheral devices of any kind (digital cameras, PDA's etc.) may be bought, installed or configured on any NCC computer without the knowledge of IS.

Disposal of IT equipment will be arranged by IS with due regard to legal (software compliance) and environmental issues, ensuring that the appropriate hardware and software registers are updated.

11 Antivirus

All NCC computers have the authorities’ approved anti-virus software installed and scheduled to run at regular intervals.

It is the responsibility of the users to report any viruses found on their computers to the IS. If a virus is discovered on a computer, IS will remove the machine from the network until it is verified as virus-free.

Users should never download files from unknown or suspicious sources. All spam emails should be deleted and unknown or suspicious attachments must not be opened.

Users should never attempt to disable their anti-virus software on their computer. If problems arise, the user should contact the IS Service Desk for assistance.

Any attempts by an employee to create and/or distribute malicious programs into the NCC network (such as viruses, email-bombs, worms, Trojans etc.) are prohibited. Any user who engages in such activity will be subject to disciplinary and/or legal action

IS cannot control anti-virus systems on third party computers. Employees are to ensure that consultants and contractors do not plug their computers onto our network without prior approval. Non- NCC employees, where possible, should make use of a NCC computer, as opposed to their own equipment. This access will be controlled via the IS Service Desk.

Employees are to inform IS of any changes to any contract that involves business partners having access to our network or infrastructure so that access can be appropriately managed.

12 Working Remotely

This part of the policy applies to your use of any NCC communications facilities whenever you are working on business away from NCC's premises (working remotely).

When you are working remotely, you must:-

- Password protect any work which relates to NCC's business so that no other person can access your work;
- Position yourself so that your work cannot be overlooked by any other person;
- Inform the Police and IS Service Desk as soon as possible if either a laptop in your possession or any computer equipment on which you do NCC work has been stolen (you will need a police crime number and report);
- Ensure that ID badges, authentication devices or memory sticks are kept separately from computer equipment when not in use.

13 Clear Desk

All confidential items (documents, CD, DVD, Data sticks, etc.) should be locked in a secure environment when the area is unattended.

No confidential information should be available for casual viewing or inspection by visitors.

All confidential documents should be placed in the confidential waste bins when ready for disposal.

All confidential documents that have been sent to a shared printer should be collected immediately and not left for casual viewing or inspection.

Any confidential notes produced during the day should be destroyed prior to going home.

14 Compliance

Compliance of this policy is subject to periodic audit. Compliance with this policy is a term and condition of your employment. Failure to comply with corporate policies is a potential corrective and/or disciplinary matter which may result in withdrawal of your access to corporate systems and disciplinary action up to and including dismissal.

All users must be aware that the organisation electronically audits all computers on a regular basis. In addition, sample random audits may be carried out.

15 Monitoring and Review

Monitoring for changes of ISO/IEC 27001 is the responsibility of the IS Compliance and Risk Officer who will ensure on-going monitoring and audit of the processes/guidance in place under the policy.

Changes to the guidance documents are the responsibility of the IS Compliance and Risk Officer but will be dependent on, for example, changes in; technology, local procedure, legislation and NCC's computer/network infrastructure.

The Chief Information Officer is responsible for monitoring the implementation and impact of this policy.

16 Contact Information

Any queries arising from this Policy or its implementation can be taken up directly with the IS Compliance and Risk Officer at ITSecurity@northumberland.gov.uk

Personal data is subject to the principles and provisions of the Data Protection Act 1998 and the Council's Data Protection Policy. Advice on the requirements of these documents is available from the Council's Data Protection Officer at data.protection@northumberland.gcsx.gov.uk.

Individuals requesting personal data held about themselves should be directed to our Subject Access Information Pack (V5) which is available to download on our Internet Data Protection Webpage.

Requests for information about the Council's services, activities and business rather than personal data should be directed to the Information Governance Officer at foi@northumberland.gov.uk

17. Associated documents:

- Mobile Computing Policy
- Data Protection Policy

- Data Quality Policy
- Internet and Email Usage Policy
- Using your own Device Policy