Information Security Policy

Helping you safeguard council information, equipment and reputation

December 2011

The council's Management Board approved this policy on 12 December 2011.

Contents

Introduction

This Security Policy document summarises what is expected of all Kirklees Council employees in the course of their duties and while on council premises.

Its aim is to protect the council's customers, employees, assets (including information assets), finances and reputation by reducing the risk of:

- Harm to individuals
- Accidental loss or damage to assets
- Unintended change to, or disclosure of, personal and confidential information
- Deliberate and harmful acts carried out through lack of awareness of their consequences

It applies to:

- All services of the council
- All employees of the council, both permanent and temporary
- Councillors
- Any other person, or organisation, working for the council or on council premises

This policy document provides the information necessary to enable staff and others to meet their general responsibility to safeguard the council's information and other assets.

Personal Data and Sensitive Data

Any reference to **personal data** in this document means private information, whether in electronic or written form, about identifiable clients, employees, members of the public or any other persons. **Sensitive** personal data includes sensitive information about a living, identifiable individual for example, information which relates to their racial or ethnic origin, political beliefs or to their physical or mental health.

Detailed Guidance

Detailed guidance on all aspects of Information Security in this policy can be found on the intranet at Information security: menu

Government Connect

Kirklees Council has been accredited as Government Connect Compliant. This means that our infrastructure, technology and working practices have been assessed as secure, and we are able to use facilities provided by Government Connect for secure information exchange between the council and central government departments. This policy forms part of our compliance with Government Connect.

For further information and advice on information security and on this policy, contact the Information Access and Security Officer

1. Organisational Security

	Responsibility
1.1. The Management Board has a central custodian role on information security matters.	Directors and Assistant Directors
1.2. Senior management teams are responsible for implementing policy and advice.	Assistant Directors and Senior Managers
1.3. The Communications Board will direct, review, support and approve Information Security campaigns, advice and overall responsibilities. Its responsibilities are: • to recognise opportunities and risks • to flag up issues of concern • to coordinate effort • to review advice	Directors and Assistant Directors
1.4. All managers and supervisors must ensure that those who report to them are aware of their general responsibilities in respect of security and the value of information, and of any issues or risks specific to their areas of responsibility.	All managers and supervisors
1.5. Information security should be a regular item on team meeting agendas to ensure that issues of concern are highlighted and addressed.	All managers and supervisors

2. Personal Security

	Responsibility
2.1. General responsibility for information security will be included in contracts of employment.	Human Resources
2.2. Checks on the career history (including criminal records) of job applicants will be made, appropriate to the responsibilities of the job.	Human Resources
2.3. Contractual arrangements with staff agencies will require similar, appropriate checks on agency staff.	Services
2.4. External contractors, consultants, trainers and others employed on council premises or given access to council systems must be subjected to checks and agreements appropriate to the services to be provided.	Employing managers
2.5. Work placements, students, volunteers, partners and any other persons not subject to the contract of employment, and having access to council premises and/or systems, will be required to sign confidentiality and security agreements.	Line managers
2.6. A record will be made of equipment, fobs, etc, issued to new employees and any of the above.	Line managers
2.7. Induction training will include security and data protection.	Line Managers
2.8. Staff will wear ID badges at all times (unless otherwise agreed in certain circumstances).	All staff
2.9. On change of employment, access to computer systems and council property issued should be reviewed and returned or cancelled where appropriate. On termination of employment, all council property must be returned or accounted for, and computer system access cancelled.	Line managers

3. Security of Information

	Responsibility
3.1. It must not be assumed that information is a common resource to be freely exchanged	All
3.2. Information is an important council asset. Much of the information held is available to individual members of the public under the terms of the Freedom of Information Act, subject to specific limitations and exemptions, in particular: • personal data, which can only be disclosed to the person it relates to, unless there is consent or a legal requirement • information held in confidence • credit cards details, which must not be disclosed nor stored on paper, on computer systems or audio tape All information, whether disclosable or not, must be protected from accidental or malicious loss and damage. Personal and confidential information must be protected from unintended access and disclosure and may only be disclosed to persons who can show they have a right to it.	All employees, councillors and contractors
3.3. Every personal data set routinely shared with an external agency must be the subject of a sharing agreement based on the corporate model adapted to the particular circumstances and the nature of the information to be shared. Each agreement will define the method of transmission and the security measures that will be employed to ensure the safe delivery of the information. IT can advise on the various methods of secure data transmission available**.** Responsible managers will rigorously enforce agreed security measures.	Managers
3.4. A central register of all data-sharing agreements and data transfers will be established and maintained by the Information access and security officer, and all existing and new agreements and arrangements will be notified to it.	Managers Information Access and Security Officer
3.5. Where there are formal data-sharing agreements with other organisations, managers must ensure that all staff are aware of the existence of any such agreements, and of their terms and scope.	Managers

3.6. Personal data should not be accessed or viewed without legitimate reason. Under no circumstances will personal data held by the council be accessed, viewed or used for any private purpose.	All employees, councillors and contractors
3.7. Personal data should be stored on shared network drives (e.g. H: or G:) and not on a PC's C: drive. If the computer is 'stand alone' (not linked to a network), any essential data must be regularly copied onto alternative secure storage. Encrypted data sticks are available from the IT helpdesk.	All employees, councillors and contractors
3.8. No personal data should be held on laptop computers or portable storage devices (e.g. data sticks, mobile phones) for longer than necessary to carry out intended tasks, i.e. it should be deleted after use or transferred to network storage. Staff should ensure they are registered to use laptop encryption if they carry personal or confidential data routinely. No encryption or password facility should be used other than as specified by IT.	All employees, councillors and contractors
3.9. Personal data transferred to a shared portable device must be removed before the device is made available to another person.	All employees, councillors and contractors
3.10. Personal and confidential information in paper files or on removable media must be stored away at all times when not in use.	All employees, councillors and contractors
3.11. Electronic transmission of personal or confidential data should be via one of the two secure email systems available within the council. • **GCSx email** – which should be used for sharing restricted and sensitive data with individuals from other public organisations (including other councils, central government bodies, NHS, police) who also have a secure GCSx email account Instructions for setting up a GCSX email account • **Anycomms** - which should be used for sharing sensitive information with any other organisation. *If you wish to use this method and either you, or the organisation you are*	All employees, councillors and contractors

transferring the information to, do not already have an *Anycomms account then please contact the IT service desk.* Ad hoc transfers of personal or confidential data to external agencies not otherwise covered by data sharing agreements should be avoided: where these are necessary then advice must be sought on the legal and technical mitigations that should be employed to protect the data, intellectual property, and to ensure the council's data protection obligations are properly met. In particular, personal and confidential data: • must not be sent for purposes of "testing" whilst individuals can be identified • must not be sent or published using instant messaging, social networks, file sharing sites, external email or fax • must not be published or stored on any internet sites, or placed in any external hosted system under "general terms"; a formal council contract must be put in place or the terms formally reviewed by Legal Services • should only then be published where managerial guidance is available. This should clearly state the purposes and scope of any such publication, with due reference to the agreed terms, the council's obligations to follow the law, professional guidance and duties to protect staff and the public from misuse of information. The sender is always responsible for verifying the intended recipients are who they say they are and are entitled to the information.	
3.12. Staff responsible for council PCs and laptops not permanently connected to the network are also responsible for regular back-up of data and for arranging for software patches to be applied and anti-virus and anti-spyware software to be regularly updated.	Managers, all employees, councillors and contractors
3.13. Documents containing personal or confidential information must be disposed of by shredding. This can be by services, through the confidential waste collection service offered by Document Solutions, or by an agency which can guarantee secure destruction. Paper containing personal data must not be recycled or used as scrap.	Managers, all employees, councillors and contractors

3.14. Documents, media, redundant PCs and similar equipment for disposal should be stored in a secure area until removed for disposal.	Managers
3.15. PCs, laptops and other devices must be disposed of through IT, which will ensure all personal data has been securely removed using specialist software. If PCs are to be re-allocated then IT will rebuild the machine in order to ensure secure deletion of any existing local data.	Managers
3.16. Data on disposable electronic media such as CDs and floppy discs, and any unwanted media containing personal data must be physically destroyed when no longer required, with due regard for personal safety, preferably using an appropriately designed shredder.	Managers, all employees, councillors and contractors
3.17. Any loss or damage to information, or equipment that may give access to information (e.g. ID cards, tokens, laptops, mobile phones , usb sticks) must be reported as soon as practicable to the IT service desk and to the Information Access and Security Officer	Managers, all employees, Councillors and contractors
3.18. Any paper records taken out of the office must be treated with care, and extra care must be taken when destroying or disposing of anything outside a council location (e.g. at home or at a partner site).	

4. Physical Security

	Responsibility
4.1. All council premises other than recognised public areas are 'controlled areas' for the purposes of implementing security policy.	Managers
4.2. Managers should be satisfied that access to the areas for which they are responsible is adequately controlled by their own or shared physical barriers or reception points.	Managers
4.3. Windows and doors allowing entry from uncontrolled areas must be closed and locked against external access when the location is unoccupied.	Managers, all employees, councillors and contractors
4.4. Visitors must be identified and supervised while inside controlled areas.	Managers, all employees, councillors and contractors
4.5. Staff should not allow unknown and unidentified persons access to any controlled area, e.g. by holding doors open. Anyone who feels unable to challenge a stranger should notify their manager or security without delay.	All employees, councillors and contractors
4.6. Computer screens should be positioned so they are not visible from outside the immediate work area	Managers, all employees, councillors and contractors
4.7. All staff must be alert to personal and confidential information in any form being visible beyond the immediate work area.	All employees, councillors and contractors
4.8. CCTV systems, where installed, must be the responsibility of a nominated person who will restrict access to recordings and ensure compliance with good practice	Managers responsible for CCTV installations
4.9. All staff must be aware of the possibility of bomb threats and premises managers must be aware of the procedure to follow. Public areas should be kept tidy so that objects out of place can be identified.	All employees, councillors and contractors

5. Computer Security

	Responsibility
5.1. Every user of a system should have their own user name and a set of rights appropriate to their work.	IT, system owners
5.2. Access to all computer applications must be controlled and protected by secure passwords.	IT, system owners
5.3. No external party, supplier, bureau, service provider or other agency may be given access to systems, data, hardware or networks unless an appropriate access agreement has been signed by them to ensure they understand their responsibilities.	IT, system owners
5.4. Passwords used to protect computer systems: • must be a minimum of 8 characters and include uppercase, lowercase and numeric characters • must not consist of purely dictionary words, personal names or words that have associations with individual users • must be changed regularly, or as required by particular systems • must not be shared with any other person • must not be written down in a manner discoverable by any other person	All employees, councillors and contractors are responsible for ensuring that their own passwords meet these standards.
5.5. Computers should be logged out or the screens locked when left unattended. A 4 digit PIN should be set on all mobile phones and PDAs and the device should lock automatically after a short period of inactivity**.**	All employees, councillors and contractors. IT
5.6. All staff using mobile equipment, i.e. laptops and smartphones must be aware of the additional and significant risks of: • theft (including theft from council premises) • loss of equipment • information 'leakage' through being overlooked or overheard or interception • the opportunity for hacking presented by Bluetooth or Wi-Fi	All employees, councillors and contractors

All staff taking information and equipment out of council premises should: • be aware of who is around when they use them • place council property away out of sight when not in use • not use Bluetooth on mobile phones and laptops • if possible use a direct cable or encrypted power line adaptor to connect to a network provider • use VPN to connect to the council network before surfing the internet • turn off Wi-Fi on return to the office and before connecting directly to the council's network.	
5.7. Working at home must be carried out with similar consideration for security as office-based working. Staff transferring personal data from council sources to their own computer, data stick or mobile phone etc are personally liable for the legal consequences. Encryption should be enabled for staff working in a mobile setting on council equipment to protect personal and confidential information wherever possible	All employees, councillors and contractors
5.8. Staff who choose to use their own home computers for ad hoc work purposes must ensure that: • they have gained the agreement of their manager • they are not in breach of any formal data handling procedures which forbid use of personal equipment • the operating system and application software are patched regularly and that anti-virus, anti-spyware, and personal firewalls are installed and up to date • family members are not able to view data • data is transferred and deleted securely at the end of a working session	All employees, councillors and contractors are responsible for ensuring these standards are met on their own computers.
5.9. Emails that are obviously spam should not be opened, but sent to the Sin Bin.	All employees, councillors and contractors
5.10. Unexpected and unsolicited attachments to emails should not be opened and similar links to websites should not be followed.	All employees, councillors and contractors

5.11. No software should be installed or executed on a council owned computer without the agreement and assistance of IT.	All employees, councillors and contractors
5.12. No hardware should be installed or attached to the council network without the agreement and assistance of IT. This includes Bluetooth and Wi-Fi adapters, personal laptops, Ipods, personal cameras etc	All employees, councillors and contractors
5.13. Live personal data must not be used in the development of new computer applications, and may only be used in testing to verify consistency of output between an old system and its replacement or to assist in the resolution of an ongoing issue when all other options have been exhausted.	IT, system owners
5.14. Anyone becoming aware of an incident or event that could compromise the security of their computer should report it to their manager. Incidents must be also reported to the IT service desk and to the Information Access and Security Officer Such incidents include, but are not limited, to: • the presence of intruders • exterior doors and windows left open inappropriately • unauthorised access or attempted access to computer systems • unauthorised access to personal data in any medium • accidental loss or disclosure of personal data • presence of a computer virus or spyware • equipment confiscated or inspected. You can raise concerns in confidence under the Whistleblowing policy.	All employees, councillors and contractors

6. More Information

Data protection	Data Protection policy statement
Information management	Information and knowledge management
Forms (including access request, employee termination etc)	Forms bank
Home working and mobile working	Working away from the office - technology to support you
Information security	Information security: menu
Personal Use (Use of Electronic Communications in the Workplace Policy)	Use of electronic communications policy
Whistleblowing	Whistleblowing
e-learning courses on information security and data protection	Learning Management System
Social media guidelines including a policy and code of conduct	Social media guidelines

7. Legal Context

Data Protection Act 1998
Defines personal data and regulates all aspects of its use and processing.

Computer Misuse Act 1990
Prohibits unauthorised access to computer material, unauthorised access with intent commit or facilitate commission of further offences, and unauthorised modification of computer material.

Copyright, Designs and Patents Act 1988
Covers the copying of proprietary software.

Regulation of Investigatory Powers Act 2000
Part III: Investigation of electronic data.