Information security acceptable use policy

Introduction

The council has a responsibility to:

- securely manage its own information assets, the information made available to it by service users, residents, business, suppliers, and all information in its care; and
- protect that information from unauthorised disclosure, loss of integrity or availability.

The policy applies to all information (both paper and electronically stored) owned or managed by the council, which is used directly or indirectly (including through contractors and sub-contractors) to deliver its services.

This policy applies to all employees of Knowsley Council and to all other persons working for the council who have access to, or use of, the council's facilities and/or equipment.

Information is owned by the council not by an individual employee.

Employees must be aware that non compliance with this policy may place the council and the information created and/or managed by the council at serious risk and may lead to disciplinary action or other equivalent sanction. This may include dismissal where the breach is considered to be sufficiently serious. In certain cases a criminal offence may be committed and this may be referred for investigation.

The following principles apply to **all** aspects of the use of the council's information. They must be read and understood by all employees.

1. Responsibilities

I **must** adhere to the corporate information security policy, this acceptable use policy and to any associated procedures. Corporate procedures which need to be followed include:

- Information Security Guidance document
- Fax procedures
- Protective Marking Scheme – especially follow guidance on how to manage and transfer 'protectively marked information'
- IT acceptable use protocol – through following the guidance on section 4.7.

2. Protection of information

I **must:**

- take reasonable measures to protect the council's information assets from unauthorised access, disclosure, modification, destruction or interference;
- handle information in accordance with its information security classification;
- follow the requirements in the Protective Marking Scheme to manage protectively marked information; and

- securely manage all information which is sensitive, personal and/or confidential.

These responsibilities are extended outside the council's premises and outside normal working hours.

I **must** return all information assets in my possession at the end of my employment with the council. This includes:

- access passes;
- hardware (laptops, PCs or smart phones);
- physical and logical access tokens (system access tokens, ID badge, keys); and
- council documents.

3. Reporting information security incidents

The term 'information security incident' is very broad and includes, but is not limited to, incidents that relate to the loss, disclosure, denial of access to, destruction or modification of our information or information systems.

The following are examples of information security incidents. This is not an exhaustive list.

- Unauthorised access or disclosure of information. This includes sending personal, sensitive and/or confidential information (electronically, by fax or in hard copy), to someone who is not entitled to receive it.
- Theft or loss of IT equipment, paper records, or computer media, for instance CD-ROMs or USB sticks.
- Use of any facilities or systems (both paper and electronic) to engage in fraudulent activities.

I **must:**

- immediately report any information security incident to my Head of Service. If my Head of Service is unavailable then I must report it to my Director or most senior manager available; and
- report all information security incidents whether I think they are trivial or not.

It is compulsory to report all information security incidents. If you feel the need to report this privately the council has a whistle blowing procedure.

4. Reporting information security weaknesses

An information security weakness is defined as an event that could lead to an information security incident.

I must report any information security weakness straight away to my Head of Service or most senior manager available.

I **must not** try to exploit the weakness in any way.

5. Security of council premises

I **must:**

- wear my ID card at all times within council premises;
- immediately inform my manager and the Building Management Assistant in Asset Management if my ID card is lost or stolen;
- assume responsibility for all visitors, escort them at all times when they are on council premises, ensure that the visitors log is completed and that visitor passes are obtained and then returned when they leave the premises; and
- ensure that windows are closed and locked when offices are unattended and at the end of the working day.

I **must not**:

- transfer my ID card to anyone else; or
- let anyone avoid or bypass security by following me or another person through an access control door, unless it is going to cause me physical harm. If you do think that you are going to be physically harmed and a person manages to gain access, inform your Head of Service or most senior manager available immediately.

6. Managing information in the office

I **must**:

- lock away protectively marked information when not required, especially when the office is vacated; and
- only print documents containing sensitive personal and/or confidential information using secure print facilities (printer mailboxes).

7. IT security controls

I **must** adhere to the controls in the IT acceptable use protocol

8. Disposal of information

I **must:**

- dispose of information securely and safely when no longer required;
- dispose of paper which contains classified information ('Restricted' or 'Protect) by either cross cut shredding or placed in a secure disposal container;
- dispose of all computers (including PCs, laptops and servers) through the IT Service; and
- contact IT if I am disposing of memory sticks, CDs, and other electronic devices when I have finished with them.

9. Transferring information externally

I **must:**

- have authority to transfer information externally;
- protect information being exchanged from interception, copying, modification, misrouting, loss and/or destruction;
- only transfer protectively marked information by approved methods;

- Only use encrypted devices (encrypted USB sticks or encrypted CD-ROMs) for all information that has been authorised for transfer by removable media;
- take reasonable measures to protect paper documents (if authorised to take outside of the council's physical environment) against unauthorised access, misuse or corruption;
- take care when using electronic messaging, such as email, to transmit any form of information; and
- ensure I am authorised to send it and/or the recipient is authorised to receive it and that the method of messaging is sufficiently secure to protect the information being sent.

I must not:

- send or forward business emails or electronic files of any sort to my home email address;
- use cloud based storage;
- knowingly leave protectively marked information on printing facilities including copiers, printers and faxes; and
- open or respond to individual transactions and/or transmitted information or e-mails if I have any suspicions about them. I must report the matter through my line manager and if necessary the IT service desk to request advice or assistance.

10. Working remotely

I **must:**

- have appropriate authorisation to take away council assets including information, equipment and software from council premises;
- have explicit approval by my line manager for removing protectively marked information if working remotely;
- give information stored or processed outside of council controlled locations the same level of protection as that which is worked on internally. This applies to remote access connections used to do work on behalf of the council, including reading or sending email and viewing internet web resources;
- take all necessary precautions to prevent loss, damage or theft of information in my care;
- ensure that encryption facilities are available and working on the IT equipment I am using once authorised to work remotely on council equipment; and
- synchronise information with the relevant centrally stored information as soon as possible, if information is processed remotely on non-networked systems.

If I **must** work on council information in a public place care **must** be taken to ensure that the work cannot be overlooked or viewed by unauthorised personnel.

I must not:

- include identifying personal information on documents used to collect personal information unless absolutely necessary.

11. Home working

I **must:**

- only take the minimum information home in order to do my work;
- have and use a secure locked storage cabinet to store paper records if I am classed as an 'at home' worker or a 'from home' worker;
- ensure that, where possible, I lock away personal or confidential information (for example information which if lost or stolen would cause an individual harm or distress);
- bring all paper documents containing personal or confidential information back to the office for secure disposal if I am an 'occasional' home worker;
- use a cross cut shredder to dispose of paper documents containing personal or confidential information if I am an 'at home' or 'from home' worker or bring the documents into the office for secure disposal;
- ensure that I keep paper documents containing personal or confidential information separate from valuable items, for example remove from laptop bags, handbags, and so on;
- ensure that when I leave my home, if council information is stored inside, I will lock all doors and windows and set a burglar alarm if one is fitted;
- only access the council network via a secure Virtual Private Network connection and using a council provided device;
- take copies of paper files or electronic documents containing personal or confidential information home rather than originals, unless there is no alternative. Dispose of the information in a secure way when no longer required;
- ensure that any device used to work at home, e.g. laptop is encrypted; and
- take all reasonable steps to maintain security of and prevent loss or damage to any information taken away from the council office environment.

I **must not:**

- include identifying personal information on documents used to collect personal information unless absolutely necessary, for example when collecting information on vulnerable people;
- leave paper or electronic files where they could be viewed by others, including family members;
- leave paper records containing personal or confidential information in the same storage bag as my laptop;
- store information on local disk drives (C:/ drive) of a PC or laptop as this is not backed up. The only exception is when there is no access to the network when saving a document. Once access to the network has been restored, the information must be saved to the correct server storage area, and then deleted from the local disk drive;
- transfer documents to work on any non council device and vice versa via a USB stick or any other removable media or any cloud based storage service (for example 'sky drive');
- write passwords down;
- put confidential or personal information in a domestic waste or recycling bin at home;
- use any device, other than one provided by the council to conduct council business;

- remove a paper file from the council unless absolutely necessary, permission has been given and it can be stored securely at home; and
- use a personal (non council) e-mail account for council business.

12. Contact details

Contact Data Protection Officer if you have any questions about this document.

Telephone: 0151 443 4660
Email: data.protection.officer@knowsley.gov.uk