Wokingham Borough Council

Information Security and Acceptable Use of ICT Policy

Date Approved: February 2014 / New format July 2016
Last Updated: March 2018
Date of Next Review: By May 2019
Policy Review and Update: Stuart Bignell
Document Marking: UNCLASSIFIED

This document requires approval from one of the following:

Sponsor Approval	Name	Signature	Date
Director of Corporate Services	Graham Ebers		
Senior Information Risk Owner (SIRO)	Sally Watkins		
Lead Specialist, Human Resources	Sarah Swindley	SS	26.03.2018

Contents

Introduction and Policy Aims

Wokingham Borough Council handles a large amount of information - financial, personal and sensitive, including information about members of the public. The Council is responsible for the protection of its information assets.

Wokingham Borough Council recognises the importance of information assets, the need to identify them, to protect them and the benefits they can bring when utilised appropriately. Unauthorised access to the council's data, IT systems and secure areas of the building can result, for example, in a serious threat to the safety of individuals, loss of financial information, breach commercial confidentiality and regulatory action from the Information Commissioners Office (ICO).

This policy defines the rules and responsibilities needed for the secure handling and protection of council information. The aim is to establish good professional practice.

What is the aim of this policy?

To ensure that all information systems operated by the council are secure and comply with the requirements of Data Protection, the Computer Misuse Act, the Caldicott Guardian principles, the principles of the International Standard for Information Security and PSN requirements.

All persons authorised to access the councils IT facilities, systems, or data must comply with these rules and procedures. The policy applies to any person accessing the councils IT facilities or electronic data in any format, on any device, and from any location.

The Council is committed to providing training and support to ensure everyone working for the council understands their responsibilities with information.

Who is this policy for?

This policy applies to Councillors, employees of the Council, contractors, consultants using the councils equipment and/or assets, agency staff, and others working in a similar capacity. It also applies to volunteers and partner organisations.

It does not cover work conducted by external consultants who independently use their own IT equipment, systems and information assets. Their Data Protection and information protection obligations must be stated in their contract for council work.

Our roles and Responsibilities

1. Council employees and others conducting business on behalf of the Council must comply with this policy.

2. Council Assistant Directors are responsible for the security of information assets (as Information Asset Owners) and are accountable for legal compliance, including to the Data Protection principles.

3. Council Directors, Assistant Directors, Service Leads and Managers are accountable for the protection of data stored on electronic assets used by their teams and others working for them. They must ensure that employees return equipment and assets issued to them before they leave the council.

   They must ensure employees and others working for them are aware of and in a position to comply with this policy. They will take agreed action(s) to reduce the risk of data breach repetition.

4. The IT Service is responsible for procurement, technical security set-up and (re-)issue of Council equipment and assets. Also for the maintenance of records held about equipment, assets and their owners.

   IMT also has responsibility for co-ordinating regular stocktakes of equipment and assets, and follow-up investigations and actions on any irregularities. They must also investigate, manage and resolve the IT aspects of incidents and breaches.

5. The Data Protection Officer is responsible for investigating any breaches reported, and oversee their resolution. They must also ensure that breaches and any improvements made are communicated to employees.

6. The Senior Information Risk Owner (SIRO) must assess the impact of personal data loss or disclosure. The SIRO can propose action(s) to reduce the risk of a breach occurring again.

7. The Information Governance Group (IGG) meet regularly to discuss areas relating to information security, including any breaches that have occurred and lessons learnt. The representatives are responsible for communicating back to teams in their area on any items raised, and help in the implementations of any actions related to IT and Information Governance projects.

8. The Council's Shared Audit and Investigations Service will review the council's performance in implementing this policy, and consequent follow-up investigations and actions.

   They must oversee the investigation of theft, and assist in liaison with the Police and provide support for Police investigations.

What happens if the policy is not followed?

Failure to follow the rules, procedures and responsibilities in this policy, may lead to action being taken in line with the council's disciplinary procedure. If a criminal offence has been committed, further action may be taken to assist in the prosecution of the offender(s).

If you do not understand the policy or how it applies to you, seek advice from your line manager, Information Governance Group representative, or from the Data Protection Officer.

Using the policy and guidance

Using equipment and information assets

Equipment must be obtained through the IT Service only and must not be ordered directly from manufacturers. The IT Service must ensure that equipment is identified by marking either with an asset tag number or with some other visible indication of council ownership. The person issuing a piece of equipment must ensure complete details are captured about the person to whom it is issued.

When an individual leaves the Council they, or their manager, must return their equipment to the IT Service by following the councils leavers' process. The IT Service will then check the equipment and update records accordingly.

If the equipment must be destroyed (or disposed of) the IT Service must ensure that its data storage area is either physically destroyed, or that data storage areas are electronically destroyed in accordance with certified security standards.

The IT Service must keep accurate and up to date transfer, destruction and disposal records, and make available for audit if required. A full equipment stocktake should be completed at least once a year.

Information Asset Owners must provide accurate and complete data about all of the equipment they have in their area when so requested.

Private business or personally owned electronic devices must never be physically connected to the council IT network. This is because of the risk of virus contamination. These devices may only communicate with the council IT network through an authorised Wi-Fi connection.

Obtain your manager's authorisation to use a personally owned device either remotely, or through the council's Wi-Fi service. For members, the nominated person is the council's Monitoring Officer. Your device will be assessed by IT Service Desk and they can explain what security set-up is required before the device may be used for council business.

How we handle information and keep it secure

The Council must provide employees and others conducting work for the council with an identity badge. It must be worn at all times whilst on council premises or on council business. You must wear a temporary badge if you forget yours. You must inform the Building Support Officers immediately if you have lost, damaged, or had your badge stolen. If you have repeatedly lost your badge you may be subject to the Council's disciplinary procedure.

The identity of any individual being contacted by, or contacting, the Council must be checked and proven before sensitive or personal information is provided to them verbally, on paper or electronically.

Individuals must ensure that as far as possible no unauthorised person has access to any personal or sensitive data held by the Council. Take precautions to avoid your screen being overseen accidentally or deliberately by unauthorised individuals.

The councils Protective Marking scheme applies to all emails, and physical documents – The exception to this rule is for court documents and committee reports. Items that contain sensitive or personal data must be given a security protective marking to define the protection needed against lost, theft or unauthorised access.

Take precautions to ensure that conversations about personal data or sensitive council matters cannot be overheard. These conversations should not be held in public places where members of the public may overhear. After listening to voice recordings (calls, interviews, etc) in the course of council business, you must not disclose what you have heard to unauthorised individuals. Care should also be taken when leaving messages on answering machines, as you do not know who may access the message.

All post received or sent by the council must be handled in a secure manner. Any post received by the council with an 'only to be opened by addressee' marking, or similar wording, must be opened by that addressee. All letters sent internally that contain sensitive personal data must be in an envelope and protected with the following marking OFFICIAL or OFFICIAL-SENSITIVE. For letters sent externally that contain sensitive personal data, they must be in an envelope with the marking 'Private and Confidential'. These markings may also be used for letters containing commercial, personal data, or other types of non-personal sensitive information.

A 'Return to sender' or 'Do Not Redirect' must be written on envelopes and/or packages sent in case the post is not correctly delivered when information being sent includes sensitive data. When sensitive personal data (special categories of personal data under GDPR), commercially sensitive, original documents, or large quantities of personal data are sent and serious damage could be caused if it were misdirected or lost, then additional protection must be considered. It is recommended that this type of information be hand delivered, sent recorded delivery, or delivered by courier.

Council documents, letters or packages delivered by hand to an individual's home, or collected in person, should only be given to a named addressee, whose identity must be verified before the item is handed over. A receipt must be signed to provide evidence that the individual has received the document, letter or package.

You must prevent unauthorised access to personal or sensitive information you print, copy, scan, or fax. Fax should only be used if there is no other alternative and a test fax should be sent to ensure the correct recipient receives the document.

Take extra precautions when working outside the council offices and transporting data between sites. Notebooks and documents should be clearly labelled with the relevant protective marking, name of individual and contact details to return, should they be lost.

For regular data transfers within a formal contract, then an Information Sharing Agreement (or Data Processing Agreement) needs to be completed. The Data Protection Officer is able to offer advice and guidance on this documentation. Any such agreement will need to be signed off by either the Caldicott Guardian or SIRO. For one-off data transfers then a Data Transfer Agreement can be completed, which

identifies what data is being transferred, the reasons for the transfer, and the arrangements for secure transfer of the data concerned. Both parties are required to sign this beforehand.

How we store and dispose of information

Data should be stored on the council's IT storage areas or systems, and if saved to the local drive, i.e. on your C drive, this should be moved to the council network at the earliest opportunity. By holding data on the council network you reduce the risk of loss, as your data will be backed up.

If an individual has access to a portable electronic device or computer media that has been supplied by the Council, such as USB memory stick, CD/DVD, camera, Dictaphone, etc then that individual is responsible for the security of the information held on that device while in transit. The information held on the device should be moved to the council network at the earliest opportunity or stored in a suitable secure storage unit.

Personal or sensitive documents must be kept out of sight when not in use, and must be locked away overnight when kept in council offices. The Council provides suitable secure storage.

The content of council safes must be recorded, and this record kept separately away from the safe. The names of employees issued with safe keys or code must be recorded. If keys are lost, stolen or the code made known to unauthorised individuals then the lock must be changed.

Personal or sensitive documents must be disposed of by using the council confidential waste service, or by cross cut shredding. Electronic devices must be destroyed using the IT Service destruction service.

Information which is no longer required (in line with the Councils retention schedule) should be promptly disposed of by deletion or destruction. Unless an audit record of versions is explicitly required, previous versions of documents should be deleted or destroyed when the final version is agreed.

When smart working and using desks

Obtain management authorisation before working outside of the council offices for the first time. Get permission to utilise any electronic equipment, software or documents. The IT Service will issue individuals with the technical means to remote work once authorisation has been given.

Be vigilant and protect council equipment and documents when walking, when travelling on public transport, or by any other means of transport. Do not take documents out of the office unless they will actually be used. Before taking legal documents out of office get approval from your manager.

When not in use, council equipment and documents must be kept out of sight, and locked away if possible. The Council uses dual authentication to securely sign in to the Councils network to remote work. Remote workers are responsible for preventing unauthorised access to council equipment or information, whether

electronically or on paper. No family members or unauthorised individuals may be given access to council IT equipment, information or documents.

Do not print information outside council offices unless absolutely necessary. Home printing is only permitted where a business case has been approved by the SIRO. Each case submitted will be assessed individually.

Authorisation must be obtained from the Data Protection Officer and the IT Service Manager before taking council equipment outside the UK.

Any theft, or loss of equipment or information, must be reported to:

- The Police if theft is suspected, and a Crime Reference Number obtained.
- The IT Service Desk in case equipment needs to be de-activated.
- The Data Protection Officer.
- Your manager.

These clear desk rules must be followed:

1. When you are at a desk

After you have planned your work, only take the items you need to use during the time you occupy the desk.

2. When you leave a desk for a short while

There is no reason to completely clear the desk if leaving it for a short amount of time, however;

- If your computer is no longer within your eyesight then you must lock the screen. If you are leaving it unlocked while speaking to a colleague within eyesight of your computer then you should minimise all open applications to prevent them being viewed.
- Check that no personal or sensitive documents are accessible. If they are, put them out of sight or lock them away. You could also hand them to a colleague for safe keeping until you return.
- Highly sensitive documents must be locked away when not in use. This includes when you are away from a desk temporarily, e.g. lunch breaks, refreshment breaks, or meetings.

3. When you vacate a desk

The desk must be left clean and completely clear, so that someone else may use it.

All office papers and documents should either be put away, or locked away if they contain personal or sensitive information (OFFICIAL or OFFICIAL-SENSITIVE). Always lock away computer devices, CD/DVDs, USBs, or other portable equipment, etc.

Anybody allocated to a fixed desk must also comply with the clear desk policy.

Using email and managing mailboxes

Only approved email accounts may be used to conduct council business. All emails sent on behalf of the Council must be clearly identified and contain the senders name, title, service and contact details. They must never be sent anonymously by individuals. Individuals must not use another individual's mail account; nor attempt to impersonate someone else.

Emails sent when conducting council business become part of the councils corporate record, even if sent from private business or personal email accounts. Council email accounts must not be used to conduct personal business or to run a private business.

All those sending emails whilst conducting council business must acknowledge their legal responsibilities. The legal status of an email message is similar to other forms of written or electronic communication and individuals must take care not to enter into any agreements that constitute a contract. If in doubt the individual must seek the advice of the councils legal and procurement advisors. Every email message sent to conduct or support council business is considered to be an official communication from the Council.

Whilst respecting the privacy of authorised email users, the Council maintains its legal right, in accordance with the Regulation of Investigatory Powers Act 2000, to monitor and audit the use of council email accounts. Interception or monitoring will be in accordance with the provision of that Act.

Access to another's employee's email is normally forbidden unless the employee has given their consent, by setting delegated authority to access their emails. If an email account needs to be accessed by another person for specific business purposes whilst they are absent then a formal request must be made with the appropriate authorisation.

In more serious situations where an allegation has been made or suspected serious breach of policy has occurred then a formal request must be made to the council's SIRO. The Shared Audit and Investigations Service must be informed of any suspected or actual breaches of email policy before any subsequent investigation begins to ensure that it is carried out in accordance with good practice.

Email and attachments may also need to be disclosed under Data Protection rights, the Freedom of Information Act 2000 or Environmental Information Regulations 2004.

Under no circumstances should users communicate material which might be deemed inappropriate or offensive. This includes information that is illegal, defamatory, abusive, obscene, threatening or does not comply with the councils Equal Opportunities Policy. Any individual who is unclear about the appropriateness of email content should consult their manager before sending the email.

Personal and sensitive information should not be sent unless protected by encryption or some other means, e.g. by using Secure Mail or as a last resort password protected documents via unsecure email. Emails sent over the public

Internet are at higher risk of interception or loss. Wherever possible, remove or redact personal data about individuals if required. If you receive an email containing personal or sensitive information that has been sent over the Internet without any protection, inform the sender that they have taken a risk. Request that they protect their email in future.

Use email distribution lists carefully. Make certain that everyone in the list is authorised to read the information you send. Use the blind copy option when you are sending an email externally to more than one private email address. When you reply to an email containing personal or sensitive information, do not use the 'reply to all' unless everyone included is authorised to receive it.

The use of PST files is no longer permitted now that the council have a cloud based storage for emails. Email should not be used for permanent storage of documents and records that need to be retained for legal/statutory reasons. These documents must be stored on the councils network.

Those using email when conducting council business must take precautions to reduce the risk of virus and malware infection. If any junk email, 'spam' or unsolicited emails are received they must be deleted without reading them. The recipient must not reply to these emails; nor open any attachments; nor click on any hyperlinks within the email; nor forward the email on to any other individual.

Using social media at work

The organisation encourages employees to make reasonable and appropriate use of social media websites as part of their work. Social media defined as any type of interactive online media that allows parties to communicate instantly with each other or to share data in a public forum, such as Facebook, Twitter, Youtube, Comments sections, Forums, Blogs, Live chat, and LinkedIn. It is an important part of how the organisation communicates with its residents and customers, promotes its services, and communication between staff.

Employees must be aware at all times that, while contributing to social media activities, they are representing the Council. Employees should use the same safeguards as they would with any other form of communication about the Council in the public domain. Employees must obtain permission from a manager before embarking on a public campaign using social media and should seek involvement from the Councils Communications team.

The Council recognises that many employees make use of social media in a personal capacity. If employees do discuss their work on social media they must include a statement along the following lines: "*The views I express here are mine alone and do not necessarily reflect the views of my employer.*"

Any communications that employees make in a professional capacity, or via their personal account(s), must not bring the Council into disrepute (eg defamatory comments), breach confidentiality (eg revealing confidential information), breach copyright (eg using someone elses image without permission) or doing anything that could be considered discriminatory, bullying, or harassment of, against any individual.

Employees should not spend an excessive amount of time while at work using social media sites, even if they claim to be doing so as part of their work. Employees should ensure that use of social media does not interfere with their other duties. Access to particular social media websites may be withdrawn in any case of misuse.

Unless it is in relation to finding candidates, those individuals who are part of the recruitment process, either through themselves or through a third party, should not conduct searches on applicants on social media. This is because conducting these searches during the selection process might lead to a presumption that an applicants protected characteristics played a part in a recruitment decision. This is in line with the organisations equal opportunities policy.

Using the internet

Your Internet access whilst doing work for the council may be used for the following:

- Obtaining information or research,
- Communicating with residents, customers and members of the public,
- Professional networking, and approved personal or professional development,
- Council electronic commerce,
- Appropriate and authorised use of social media networking sites.

This list is not exhaustive and other reasons may apply, but must be authorised.

You are responsible for the content and security of everything you send to or receive from the internet. The Internet is a primary source of virus infection, and you must always check whether sites are safe/secure to access. If software needs to be downloaded from the Internet onto council IT equipment please submit an IT request form.

Internet communications are not guaranteed to be safe, and messages may be lost or intercepted. Send personal and sensitive information only to Internet sites that are protected (i.e. with an Internet address starting ‘https’ and with a padlock symbol shown at the bottom of the screen).

Personal use of council Internet is normally restricted to non-work time, e.g.:

- before 08:45;
- during lunchtime between midday and 14:30 and;
- after 17:15 on Mondays to Thursday, or after 17:00 on Fridays.

At the discretion of your manager, and provided it does not interfere with your work, limited personal use of the Internet in work time is permitted. The purchase of personal goods or services is permitted using the councils Internet during non-work time.

Internet access, including social media access, and security using the council owned Internet will be monitored. The Council has a responsibility to ensure that use of its Internet facilities complies with legislation and statutory guidance. Internet from the council’s IT network are owned by the Council. All access is recorded, logged and may be used for the purposes of:

(a) monitoring total usage to ensure business use is not impacted,
(b) monitoring access to websites and appropriate usage.

Members of the public, and others doing council work, using council owned Internet are protected by having access to certain categories of websites blocked. Examples of blocked categories include but are not restricted to:

- Illegal;
- Pornographic;
- Violence;
- Hate and discrimination;
- and Offensive Web content.

If you need access to any blocked categories of information using council owned Internet facilities, get your manager's authorisation and contact the IT Service Desk.

If you think you have a virus infection, immediately unplug, and disconnect the wireless on your computer. Any concerns, messages or warnings relating to viruses received when using council owned Internet facilities must be referred to the council's IT Service Desk.

If you know of any council Internet misuse that conflicts with this policy or with the Equal Opportunities Policy you must report it to the manager responsible for the work, or submit a 'Report an Information Security Incident or Breach' form as soon as possible.

Understanding incidents and breaches

A security incident is defined as, 'any event that may threaten or cause a security breach'. An incident report must be submitted after a breach, or if there is a concern about the possibility of a future security breach. Before reporting, steps should be taken to retrieve the data where possible and prevent misuse of data.

Incidents may be reported in several ways and must be reported as soon as possible after it is discovered or anticipated. This must be done using the electronic 'Report an Information Security Incident or Breach' form on the councils intranet site. They may also be reported by telephone or verbally to the Data Protection Officer, or by emailing Information.Security@wokingham.gov.uk if more urgent and need immediate attention. The individual may also report it to their line manager.

When a 'Report an Information Security Incident or Breach' form is submitted, a reference number will be issued and the Data Protection Officer will investigate the matter. The Assistant Director for that area will be notified once the investigation is completed and briefed on the outcome. Where a reportable breach has occurred (ones which require reporting to the ICO) the Chief Executive will be notified.

A summary of the breaches and reportable breaches will be shared with the IGG, CLT and learning will be shared with the service involved and on the councils Intranet. The Shared Audit & Investigation Service will be provided a more detailed copy should this be required.

It requires that actual or suspected security incidents are reported, and reported in a timely manner. Incidents and breaches will be prioritised, investigated, and action taken to minimise any actual, or potential, risk to the public and the council.

Related Policies, Guidance, and Regulatory Obligations

Your attention is drawn to the Conduct & Personal Behaviour Guidance, Health and Safety Guidelines, Human Resources Policies and Guidelines and all other policies referred to within Wokingham Borough Councils.

In addition to the Councils policies and guidelines there are also related legal and regulatory obligations; Civil Contingencies Act 2004, Companies Act 1985, Computer Misuse Act 1990, Copyright, Designs and Patents Act 1998, Data Protection Act / EU GDPR, Freedom of Information Act 2000, Regulation of Investigatory Powers Act 2000 and International Standard for Information Security Management.

Any Other Information

The ICO periodically publishes updates, advice and guidance in relation to Information Governance. https://ico.org.uk/