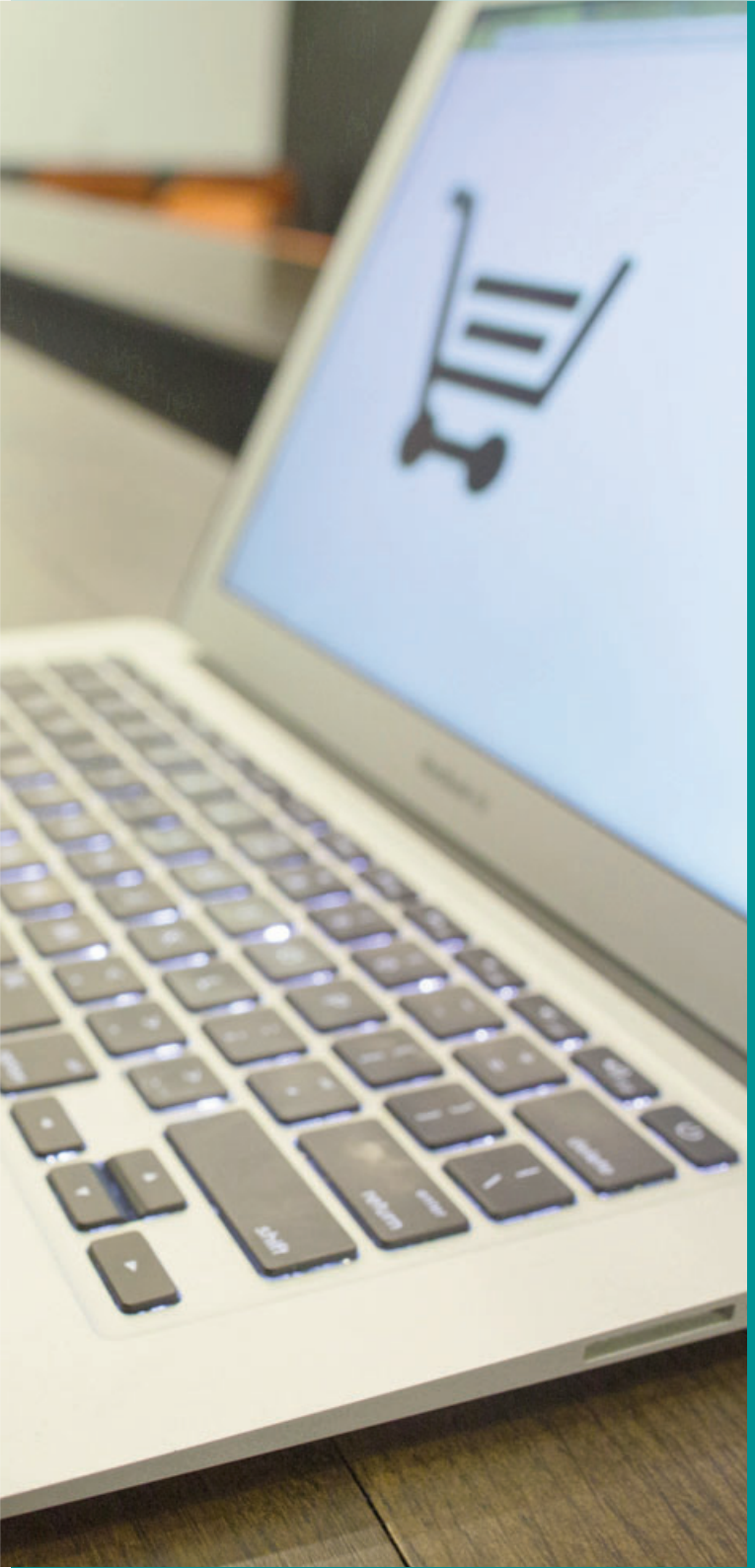


Appendix A

Tewkesbury
Borough Council

IT policy
2019

March 2019

IT policy

> “These rules are designed to **minimise the legal risks** to the council when its employees use its ICT resources.”

Introduction

This policy has been produced for all individuals who use any of the Information and Communication Technology (ICT) provided by Tewkesbury Borough Council (the council) and provides guidance on the acceptable use of our ICT.

The purpose of this ICT policy is:

- To ensure IT is used effectively.
- To protect the council
- To protect all employees and members
- To help buy, support and use IT.

These rules are designed to minimise the legal risks to the council when its employees use its ICT resources. Where something is not specifically covered in this policy, employees should seek advice from their line manager.

Ownership

All ICT equipment, services and intellectual property created by the council is stored or transmitted on our ICT infrastructure (ICT resources) are the property of the Council unless there is an agreement to the contrary. The Council reserves the right to monitor and access all information stored or transmitted on it in ways that are consistent with all relevant legislation, good practice and guidance.

Scope

This policy applies to all permanent and temporary employees, elected members, contractors, consultants, secondees and other individuals who have access to our ICT resources whether on council premises, other places of work, online, home or otherwise working remotely.

General principles

1) Ensure that you treat our ICT resources sensibly, responsibly, lawfully, and in ways that are consistent with your duties and with the council’s policies, procedures and values.

2) Email/messaging/other online communication services are an easy and effective means of communication however it isn’t, in general, a secure method. Where personal or sensitive information is to be transmitted, this must be done so in a secure way, such as password protected document with the password communicated separately to the original communication. Also, the contents of an email can be made available under Access to Information obligations and/or may be used as evidence in legal proceedings so think very carefully about what you write before you send anything. Care should be taken to verify the recipient before sharing. It is recommended that you do not use your work email address for personal business.

3) Downloading, copying, possessing and distributing information or other information from the internet or through email/ messaging may be subject to copyright or intellectual property rights. If you are unsure whether these apply, please contact One Legal;

4) Use of our ICT resources must be restricted to business and acceptable non-business use as defined below.

5) All online services must be used and shared only with the individuals in scope as defined above. Sharing of personal data should only be carried out where there is a lawful basis to do so and if it is systematic sharing, a data sharing agreement in place. If you require a data sharing agreement please contact One Legal;

6) Only equipment specifically authorised by the ICT Operations Manager within the council must be used for business use;

7) The security of user names and passwords are your responsibility and must never be shared. You are responsible for ensuring the confidentiality of information accessed via the ICT resources.

IT policy

> “If you are in any doubt about how you may make personal use of the council’s ICT resources you must **consult your line manager**”

Acceptable use policy

Employees and members must use our ICT resources to support the work of the council. However, we also recognise that there are benefits to be gained by allowing employees and members to make limited personal use of our ICT resources. All use of our ICT resources must be consistent with this Acceptable Use Policy.

- **Business use**
  This is defined as the day-to-day use of ICT resources necessary to do your work.

- **Acceptable non-business use**
  This use is confined to outside of your normal or agreed working hours. However, brief, personal use of ICT resources during working hours is acceptable, provided that such use does not interfere with, or take priority over, your work responsibilities.

  The council trusts employees not to abuse this latitude given to them, however, if this trust is abused it reserves the right to alter the policy in this respect.

  If you are in any doubt about how you may make personal use of the council’s ICT resources you must consult your line manager.

- **Misuse**
  This includes excessive web browsing or other excessive personal use of ICT resources that is considered by your line manager to be taking priority over work responsibilities, unsolicited emails, personal downloads and using our ICT resources to run a private business.

  Disciplinary and/or legal action may be taken in cases of misuse of our ICT resources as set out in out in the Disciplinary Procedure. In the most serious instances gross misconduct may result in dismissal.
  Members of the council are required to comply with the council's Code of Members' Conduct which includes provisions on the treatment.

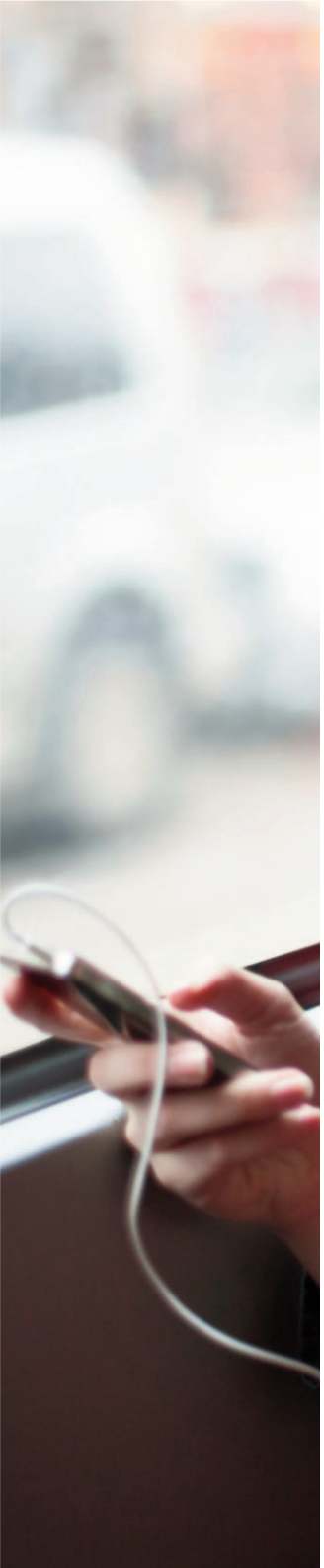
Monitoring

We reserve the right to monitor the use of our ICT resources, and access any information stored on our ICT resources, in ways that are consistent with relevant legislation and good practice.

Such monitoring may include email, internet, telephone, mobile telephone and electronic file storage use.

- **When and how will email be monitored**
  Emails may be accessed or monitored when the council considers it has a valid reason to do so. The following are examples of valid reasons for checking an employee's email:

  - If the employee is absent for any reason and communications must be checked for the smooth running of the business to continue.
  - If the council suspects that the employee has been viewing or sending offensive or illegal material, such as material containing racist terminology or nudity.
  - If the council suspects that an employee has been using the email system to send and receive an excessive number of personal communications.
  - If the council suspects that the employee is sending or receiving emails that are detrimental to the council and its partners.
  - If the council considers the email may contain anything that may affect the ICT infrastructure, such as a virus, malware, spyware, ransomware, key logger, etc.



IT policy

> “ Workers have a **number of rights in relation to their data**, including the right to make a subject access request ”

When monitoring emails, the organisation will, save in exceptional circumstances, confine itself to looking at the address and subject heading of the emails. Employees should mark any personal emails as such and encourage those who send them to do the same. Where possible, the organisation will avoid opening emails clearly marked as private or personal .

All users must notify the IT department of any security incidents and breaches immediately.

Data protection

Monitoring or accessing personal emails is in the council's legitimate interests and is to ensure that this policy on email/messaging/online communications and internet use is being complied with and/or the security of council ICT infrastructure. Monitoring or accessing personal emails may also be carried out where it is a task vested in the authority or a task carried out in the public interest such as for the prevention and detection of crime or fraud. For further information about how the data will be used please see the council’s Privacy Notice.

The officer responsible for overseeing this policy is the ICT Operations Manager.

Monitoring will normally be conducted by the council's ICT team. The information obtained through monitoring may be shared internally, including with members of the HR team, Head of Service (or above) and IT staff if access to the data is necessary for performance of their roles.

However, information would normally be shared in this way only if the council has reasonable grounds to believe that there has been a breach of the rules set out in this policy.

The information gathered through monitoring will be retained only long enough for any breach of this policy to come to light and for any investigation to be conducted. Data is normally securely destroyed in line with the ICT data retention policy.

Information obtained through monitoring will not be disclosed to third parties (unless the council is under a duty to report matters to a regulatory authority or to a law enforcement agency).

Employees and Members have several rights in relation to their data, including the right to make a subject access request and the right to have data rectified or, in some circumstances, erased. You can find further details of these rights and how to exercise them in the council's data protection policy. If Employees and Members believe that the council has not complied with their data protection rights, they can complain in the first instance to the council’s Data Protection Officer and if they are still dissatisfied to the Information Commissioner.

Information Commissioner's Office Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

IT Manager
phone: 01684 272158
email: Iain.stark@tewkesbury.gov.uk