Procedure for securing and investigating the content of council ICT equipment

1. Scope

This procedure applies to all users of the council's ICT equipment. ICT equipment includes, but is not limited to:

- Laptops,
- Mobile devices, e.g. mobile phones and tablets,
- Portable media devices, e.g. memory sticks, external hard drives, DVDs
- Remote working equipment.

Where there is a suspected breach of the law, or any council policy (including but not limited to the council's Information Management and Security policies) users should have no expectation of privacy regarding their use of any council device or the storage of any data on council systems or servers
Any council device used, and any data processed by users, remains the property of the council and may be accessed at any time by the council to ensure compliance with its statutory, regulatory, and internal policy requirements.

2. Related policies and procedures

- Code of Conduct for Employees.
- Disciplinary and Dismissal Procedure
- GFRS Service Order no. 25: Disciplinary and Dismissal Procedure
- Internet and Digital Communications Policy
- ICT Equipment Policy
- Information/IT Access Policy
- Information Security Policy
- Data Protection Policy
- Social Media Policy

The above policies are available at Information Management and Security Policies.

3. Relevant legislation

Computer Misuse Act 1990

This is the primary legislation addressing unauthorised access and misuse of computer systems. It includes:

- Unauthorised access to computer material (e.g. basic hacking)
- Unauthorised access with intent to commit further offences
- Unauthorised modification of computer material (e.g. spreading malware, deleting data)
- Making, supplying or obtaining tools for misuse (e.g. hacking tools)

Data Protection Act 2018 (incorporating UK GDPR)

This governs the lawful processing of personal data. Misuse of devices to access, share, or store personal data unlawfully can lead to:

- Regulatory action by the Information Commissioner's Office (ICO)
- Criminal prosecution for deliberate breaches

Copyright, Designs and Patents Act 1988

This law protects intellectual property, including software and digital content. Misuse includes:

- Copying or distributing software without a licence
- Downloading or sharing copyrighted media unlawfully

Communications Act 2003

Section 127 makes it an offence to send grossly offensive, indecent, obscene or menacing messages via public electronic communications networks. This includes:

- Misuse of mobile devices or computers to send abusive messages
- Cyberbullying or harassment

Investigatory Powers Act 2016

This governs the powers of public bodies to carry out surveillance and interception of communications. Misuse of devices to intercept or monitor communications unlawfully may breach this Act.

Malicious Communications Act 1988

This covers the sending of threatening or abusive messages with the intent to cause distress or anxiety. This includes messages sent via email, text, or social media.

4. Procedure

a) Following the receipt of an allegation of misconduct that references the potential use of any council ICT equipment/mobile device, the council will undertake an investigation to determine the validity of that allegation. This will include any council owned mobile device where the employee has also been authorised to use the equipment for personal use.

b) Where there is an allegation of professional misconduct that references the use of **personal** ICT equipment/mobile device(s), the council may, dependent on the allegation, liaise with the appropriate authorities, e.g. the police, to safeguard the integrity of any potential evidence.

c) On receipt of an allegation, any relevant piece(s) of ICT equipment/mobile device(s) may be taken from the employee by a senior member of staff or a member of Human Resources (HR). The equipment will then be placed in locked storage until such time as it can be reviewed. The employee's system(s) access privileges should also be reviewed by the relevant service area (in conjunction with HR/D&ICT/IMS) at this point by raising a security investigation ticket on ServiceNow. This may mean their access is then suspended for the duration of the investigation, if this is deemed appropriate, to safeguard the integrity of the investigation.

d) A senior service manager, advised by HR, will appoint an investigating officer to undertake the investigation. This will normally be an appropriate service manager, or a manager from outside of the service, depending on the circumstances of the case. The investigating officer will be bound by the council's Information Management and Security policies and the council's Code of Conduct for Employees throughout the duration of their investigation and should seek to safeguard any personal information they may become privy to as a result.

e) If the allegation relates to the use of a specific piece of software, the investigating officer will liaise with D&ICT and the system owner to ensure they understand how the software works before beginning that part of their investigation. Any training or testing will be carried out on a different corporate device. Where necessary, a

request for specialist system specific support, e.g. from a system administrator, should be sought in advance from the system owner.

f) Any interrogation of the ICT equipment/mobile device by the investigating officer will be done in the presence of a third party, usually a member of D&ICT or IMS staff. This individual will be responsible for providing a challenge to access if appropriate, and to prevent any accidental deletion or impairment of evidence by the investigating officer. This two-person approach serves to safeguard the integrity of both the investigation and the investigating officer.

g) On completion of the investigation, the investigating officer should complete a report outlining their findings and the conclusions that have been reached in line with the relevant Disciplinary and Dismissal Procedure.

h) Where the outcome of the investigation indicates improper behaviour or misconduct by an employee, the relevant Disciplinary and Dismissal Procedure will be implemented. In such cases consideration may be given to the service retaining the device rather than returning it to the employee.

i) Any ICT equipment/mobile device(s) that has been seized will be returned as soon as the investigation timeline allows.

Document Control

Document information

Owner:	Jenny, Grodzicka, Head of IMS and Data Protection Officer
Author:	Kirsty Benzie, Assistant Head of IMS
Reviewer:	Kirsty Benzie, Assistant Head of IMS; Eleanor Hutchison, Head of HR
Board(s) consulted:	
Date created:	April 2020
Next review date:	June 2028
Approval:	Head of IMS
Date of approval:	
Scheme of Delegation ref:	DPPG1
Version:	2.0
Classification:	

Version History

Version	Version date	Summary of Changes
1.0	April 2020	First version
2.0	June 2025	Major revision - the following was added: Relevant legislation section Guidance on the governance surrounding the handling of personal information during an investigation Guidance on the possibility of limiting system access

Review

This procedure will be reviewed as it is deemed appropriate, but no less frequently than every 3 years.

Contact Us

Post: The Information Management Service
Gloucestershire County Council
Shire Hall, Westgate Street
Gloucester, GL1 2TG

Email: dpo@gloucestershire.gov.uk

Phone: 01452 324000