Gloucestershire County Council
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.

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. 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) 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.

c) 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.

d) If the allegation relates to the use of a specific piece of software, the investigating officer will liaise with ICT/Information Management Service (IMS) officers as appropriate 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.

e) 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 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.

f) 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.

g) 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.

4. Review and Revision

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

5. Document Control

Author:	Kirsty Benzie: Assistant Head of IMS
Owner:	Jenny Grodzicka: Head of IMS and Data Protection Officer
Document Number:	V1.0

Revision date	Summary of Changes	Changes marked

Document Approvals

Version	Approved by	Date
Version 1.0	Assistant Head of HR Head of IMS	April 2020