ICT Policy Review

1. Summary

1.1. The ICT Policy Framework was originally approved in 2017 with the most recently amended version implemented in November 2022. This report presents further revisions, the addition of Section 17 Cyber Security Policy and the division of the policy into two parts – policies relevant to end users (Annex 2) with the more technical policies (Annex 3) in a separate document. Both documents will be available to all staff and members.

Recommendation that:	**a Members review and approve the proposed amendments to the ICT Policy.**

2. Background

2.1. Our ICT service underpins all aspects of the Authority's operation. Use of technology is essential to running modern and efficient services. Our reliance on ICT for day-to-day operations means that comprehensive policies governing the appropriate use of these resources is essential.

2.2. As technology is ever evolving, security requirements to protect our systems and data are also required to evolve to ensure that our data is protected.

2.3. The policy revisions presented are the inclusion of a specific section on Cyber Security, previously this was threaded throughout the Policy document, this remains the case, but a dedicated section is now included.

3. Policy Context

3.1. It is important the ICT Policy is regularly reviewed; although much of the policy is technical, the process of approval by members should provide assurance that the ICT policy framework is being actively managed by officers.

3.2. Artificial Intelligence (AI) and the use of tools containing an element of AI is an emerging area for the Authority. Any use of AI should be consistent with the policies presented here but they also raise a number of other potential issues, including but not limited to disclosure of the provenance of AI generated content, risks around data access and quality/review processes. A standalone AI policy is currently under development as the Authority works to understand better the potential uses and risks of AI.

4. Options

4.1. Members can consider the policies and accept them as set out or request amendments. Any substantive amendment would require further consultation with the ICT Manager.

5. Proposals

5.1. The proposed version has minor amendments and a new section on security measures and staff security training. The proposed amendments are detailed in Annex 1. The ICT Policy Framework Version 2.0 is detailed in Annex 2.

6. Stakeholder consultation

6.1. Staff have been consulted on the policies as presented with any feedback reflected in the versions set out for approval.

7. Demonstrating Best Value

7.1. There are no best value implications as a direct result of this report.

8. Finance Considerations

8.1. There are no financial implications as a direct result of this report.

9. Risk

9.1. It is important that the policies cover all material aspects of ICT functions and that these are adhered to. Should Members not approve the ICT Policy, the old policies will remain the authorised version; governance arrangements will be less up to date, which increases the risk of important processes and procedures not being adhered to.

10. Legal Considerations

10.1. Policy will ensure we continue to protect sensitive data and maintain our ability to respond to requests such as Subject Access Request and Freedom of Information.

11. Human Resources

11.1. There are no staffing implications as a direct result of this paper. If approved the amended ICT Policy will be required to be adhered to by all ICT users.

12. Diversity Implications

12.1. Some security measures may impact on staff/members with special access requirements, where this is the case, specific exceptions to general policy will be made while retaining a reasonable security baseline.

13. Sustainability

13.1. There are no significant environmental, economic or social effects as a direct result of this report.

Author/Post	Frank Blackburn, ICT Services Manager Peter Notley, Head of Resources
Responsible Officer	Gavin Capstick, Chief Executive
Date Written	15 August 2025

Annex 1: ICT Policy - Amendments

Summary of changes and additions to previous policy -

Section	Previous Version	Version 2.0 (this update)
Document Structure	Single unified policy document.	Split into Corporate ICT Policies and End User Policies.
Cyber Security Policy	Implicit throughout various policies	New section pulling together all relevant cyber elements into one section; covering risks, roles, controls, and incident response, travel abroad
Privileged Access	Not explicitly defined.	Requires separate account, quarterly reviews, and logging.
Network Monitoring	General mention.	Clarifies tools, scope, and confidentiality.
Secure Data Transmission	Not emphasized.	Encryption required, CDs/DVDs prohibited, Microsoft 365 promoted.
Patch Management	Ad hoc or undocumented.	Weekly updates, emergency patching, manual for critical systems.
Asset Management	Legacy tracking.	Uses Microsoft Intune, monthly audits, redeployment.
Change Control	Minimal guidance.	Defines change types, approvals, rollback plans.
Retention and Backup	On premise with tape	Backups retained ~3 months, external media restricted.