



REPORT TO:	Cabinet
DATE:	16 July 2024
SUBJECT:	Officer and Member ICT Policies
PURPOSE:	To seek Cabinet's approval for the proposed ICT Policies for Officers and Members
PORTFOLIO HOLDER:	Councillor Jim Astill, Portfolio Holder – Corporate and Communications
REPORT OF:	James Gilbert, Assistant Director - Corporate
REPORT AUTHOR:	Corey Gooch – Business Intelligence and Change Manager
WARD(S) AFFECTED:	N/A
EXEMPT	No

SUMMARY

ICT policies require regular review to ensure they reflect best practice and take into account technological advances, user requirements and security threats.

The ICT policies at SHDC were last refreshed in 2022 so the proposed policies represent a complete review and update. The opportunity has been taken to seek further alignment in officer policies across the South & East Lincolnshire Councils Partnership; with some variation for Councillor policy based on local requirements by this Council.

The Policies have been developed by Public Sector Partnership Services, as the Council's ICT provider.

The policies will require approval at Cabinet following consideration by the Policy Development Panel.

RECOMMENDATIONS

- That the Cabinet approve the policies set out in this report.

REASONS FOR RECOMMENDATIONS

- To ensure that the council has robust and effective ICT policies in place.

OTHER OPTIONS CONSIDERED

- None. The existing ICT Policy set requires review.

1. REPORT

1.1. SHDC's ICT Policies are due for refresh. The policies were last refreshed in 2022 and since that time the ICT landscape has changed, meaning the policies need to be updated to reflect the latest technological advances, user requirements and security threats.

1.2. The key changes to each policy are as follows.

1.3. Acceptable Usage Policy – Employees

- We have decoupled the previous Acceptable Usage Policy into two separate policies, one for Members and one for Employees.
- We have included the policy direction from the ICT Remote Working Policy into this policy to allow for the Remote Working Policy to be removed from publication.
- Guidance on the use of social media has been expanded, including the need for a social media blackout in the event of a potential or confirmed Cyber Security attack.
- Guidance on the use of email etiquette has been expanded.
- Guidance around the communications in the event of a cyber incident has been included.
- Rebranded onto a new template.
- General review of the wording and content to ensure that the information contained in the policy is current and that the emphasis on the policy requirement is clearly articulated.

1.4. Acceptable Usage Policy – Members

- We have included the policy direction from the ICT Remote Working Policy into this policy to allow for the Remote Working Policy to be removed from publication We have decoupled the previous Acceptable Usage Policy into two separate policies, one for Members and one for Officers
- Guidance on the use of social media has been expanded, including the need for a social media blackout in the event of a potential or confirmed Cyber Security attack.
- Guidance on the use of email etiquette has been expanded.
- Rebranded onto a new template.
- General review of the wording and content to ensure that the information contained in the policy is current and that the emphasis on the policy requirement is clearly articulated.

1.5. ICT Removable Media Policy

- Rebranded onto a new template.
- General review of the wording and content to ensure that the information contained in the policy is current and that the emphasis on the policy requirement is clearly articulated.

1.6. ICT Third Party Supplier Access Policy

- Rebranded onto a new template.
- General review of the wording and content to ensure that the information contained in the policy is current and that the emphasis on the policy requirement is clearly articulated.

1.7. ICT Systems Acquisition Development and Deployment Policy

- Rebranded onto a new template.
- General review of the wording and content to ensure that the information contained in the policy is current and that the emphasis on the policy requirement is clearly articulated.

1.8. The policies appended to this report are:

Appendix	Policy Name	Policy Purpose
Appendix A	ICT Acceptable use policy - Officers	To provide guidance on the safe and approved ICT use across the Authority for Officers.
Appendix B	Removable Media Policy	To provide guidance on the use of removable media.
Appendix C	Third Party Access Policy	To provide Officers with guidance to ensure the safe and compliant connectivity of third-party suppliers to the corporate network.
Appendix D	Systems Acquisition, Development & Deployment Policy	To provide Officers with guidance to ensure the effective procurement, development, and deployment of software into the corporate network.
Appendix E	ICT Acceptable use policy - Members	To provide guidance on the safe and approved ICT use across the Authority for Members.

EXPECTED BENEFITS TO THE PARTNERSHIP

Consistency in ICT Policy across the Partnership workforces is important particularly as officer teams work more closely together. In the future the Councils may also source single ICT systems to support the delivery of services and common ICT policies facilitate this.

IMPLICATIONS

SOUTH AND EAST LINCOLNSHIRE COUNCIL'S PARTNERSHIP

As identified in 'Expected benefits to the Partnership.'

CORPORATE PRIORITIES

N/a

STAFFING

The Policies will have a direct impact on the management of the workforce and ICT system. The Policies developed are in line with IT best practice and security requirements, whilst also seeking to ensure flexibility for users.

CONSTITUTIONAL AND LEGAL IMPLICATIONS

These policies fall outside of the Policy Framework of the Council and approval is an executive function. The policies will therefore be presented to Cabinet for approval.

DATA PROTECTION

ICT Policies form part of our key controls in ensuring safe storage and use of data, which includes personal data protected by data protection legislation. Taken together with other measures (such as site security, staff training, and so on) they form part of our technical and organisational measures required for compliance with UK GDPR.

FINANCIAL

The financial implications of any system upgrades that may be required will be considered and budgeted for at that time.

RISK MANAGEMENT

Adoption of suitable policies on the use of ICT is a key means of managing the risk of issues such as data loss, inappropriate access to data, and maintenance of key services that are heavily dependent upon technology. A risk register is in place in relation to ICT and this is monitored via the ICT Strategy Board.

STAKEHOLDER / CONSULTATION / TIMESCALES

Consultation will take place with the Councillor ICT Working Group.

REPUTATION

Having robust ICT policies, with a strong focus on protecting the integrity and security of data is important to the reputation of the Council, which is entrusted with sensitive client information to enable the delivery of its services.

CONTRACTS.

None

CRIME AND DISORDER

None

EQUALITY AND DIVERSITY/ HUMAN RIGHTS/ SAFEGUARDING

None

HEALTH AND WELL BEING

None

CLIMATE CHANGE AND ENVIRONMENTAL IMPLICATIONS

None

ACRONYMS

PSPS – Public Sector Partnership Services

APPENDICES	
Appendices are listed below and attached to the back of the report: -	
Appendix A	ICT Acceptable use policy - Officers
Appendix B	Removable Media Policy
Appendix C	Third Party Access Policy
Appendix D	Systems Acquisition, Development & Deployment Policy
Appendix E	ICT Acceptable use policy - Members

BACKGROUND PAPERS	
Background papers used in the production of this report are listed below: -	
Document title	Where the document can be viewed
N/a	

CHRONOLOGICAL HISTORY OF THIS REPORT	
Name of body	Date
N/a	

REPORT APPROVAL	
Report author:	Corey Gooch - Business Intelligence and Change Manager
Signed off by:	James Gilbert, Assistant Director - Corporate
Approved for publication:	Councillor Jim Astill, Portfolio Holder – Corporate and Communications