ICT and Digital Policies

Cabinet	26 September 2024
By	Hannah Thorpe, Head of Strategy and Transformation
Cabinet Portfolio Member	Cllr Rick Everitt, Leader of Council
Key Decision	No
Decision classification	Report Unrestricted, Reports Exempt
Call in status	N/A
Ward:	N/A

Purpose of the Report

To request Cabinet approval of four updated ICT and Digital policies: Acceptable Use Policy; Cyber Security and Cyber Attacks Policy; Digital Security Policy; Payment Card Industry Data Security Standards (PCI DSS) compliance policy.

This follows consideration by the General Purposes Committee (GPC) at an Extraordinary meeting on Tuesday 30 July 2024, and a subsequent 30 day consultation with staff and the council's recognised trade unions. The policies have also been considered by the new Cyber Security Cabinet Advisory Group at the inaugural meeting held on Tuesday 10 September 2024.

Cabinet is asked to approve the policies after which they will be implemented and rolled out across the organisation.

Recommendation(s):

To approve the following policies for implementation across the organisation: Acceptable Use Policy; Cyber Security and Cyber Attacks Policy; Digital Security Policy; Payment Card Industry Data Security Standards (PCI DSS) Compliance Policy.

1. Summary of Reasons

1.1 The reasons for this recommendation are to ensure that the council's overall cyber security and management of Digital and ICT are optimised by:

- Providing comprehensive guidance to officers and councillors
- Demonstrating the robust and comprehensive measures that the council takes
- Setting out regular reviews of the policies to ensure guidance is updated and reflective of best practice.

2. Background

2.1 The council's ICT provision was previously managed by an East Kent Services ICT shared arrangement (EKS ICT). A decision was taken by the three east Kent councils involved to disband this service and bring the ICT function and teams back in-house to each council. The majority of the ICT service moved back to the councils in April 2023, with the final element of the service, Information Security, being brought back in-house from April 2024. The process to disaggregate this service is ongoing and reflects the complexities of separating out the formerly interlinked systems and dependencies across the east Kent network. The process is 92% complete.

2.2 Over and above this, a review of ICT Cyber Security was conducted by East Kent Audit Partnership (EKAP), the findings of which were shared with council officers on 5 December 2023. As part of the audit, management actions were agreed regarding the council's cyber and digital preparedness and processes, which included a recommendation to review and update the council's suite of ICT and Digital policies. This reflected the fact that the policies had been created under the former shared service arrangements and required updating.

2.3 A cyber security incident in January 2024 further highlighted the need for an urgent review of the council's associated policies and procedures.

2.4 As such, the Head of Strategy and Transformation, working with the Head of ICT for East Kent Services, has been leading the implementation of the agreed management actions in order to improve the council's overall cyber and digital security.

2.5 As part of this activity, the council's Policy Manager, as directed by the Head of Strategy and Transformation, embarked on a review of existing Digital and ICT Policies with the key findings that:

- There were 14 ICT and Digital policies in total with significant overlap and duplication.
- Policies dated from the tripartite East Kent council arrangements and had been written as such.
- Policies did not appear to have been updated or notably reviewed since early 2020.
- Many processes appeared out of date, incomplete, or unclear.

It was therefore agreed that a full update of existing policies was required to be coordinated by the Policy Manager.

3. Relevant Issues

3.1 A working group was formed which included the Head of Strategy and Transformation, the Head of ICT for EKS, the Acting Digital Transformation Manager, the Policy Manager and wider Digital and ICT colleagues, to develop new refreshed policies.

3.2 They have been condensed into four new overarching policies. They are:

- Acceptable Use Policy: this sets out the expectations and requirements of any members of staff, councillors or other stakeholders using council-owned ICT equipment.
- Cyber Security and Cyber Attacks Policy: this covers the management and mitigation of cyber breaches or attacks.
- Digital Security Policy: this covers the council's digital security governance, responsibilities, risk management and operational processes.
- Payment Card Industry Data Security (PCI DSS) Compliance Policy: this sets out the requirements for ensuring that the organisation complies with the standards.

3.3 These policies have been designed to:

- incorporate current council working practices as of the current situation
- harmonise our approach, with duplication removed and clarity provided
- address the concerns flagged in the 2023 Audit Report; and
- be in line with national best practice across the ICT/Digital policy suite including by using the National Cyber Security Council's (NCSC) Cyber Assessment Framework (CAF) in the Cyber Security/Cyber Attacks Policy while anticipating future change.

3.4 In addition to the working group, feedback has been sought from:

- all Digital and ICT colleagues
- Information Governance and Equalities Manager
- PCI Compliance Officer
- Insurance and Risk Officer.

3.5 The policies were presented to the Corporate Management Team on 11 June 2024 with a request for a three week CMT scrutiny period. The feedback from this period was:

- PCI DSS Compliance to become a standalone policy in recognition of its specific and technical focus (it had initially been included within the Digital Security Policy as part of the policy refresh programme).
- A simplified one page introduction designed to incorporate the key messages to be added to all policies in recognition of the complexity of some of the policy content.
- The addition of a detailed glossary to be added to all policies incorporating references to terms throughout the full ICT/Digital policy suite.
- Further sense checking and content editing to be undertaken to aid the reader.

These changes were subsequently made.

3.6 Due to the potential disciplinary context of serious breaches of the policies and the subsequent change to an employee's terms and conditions, the policies were considered by the General Purposes Committee at an Extraordinary meeting held on Tuesday 30 July 2024. GPC noted/approved the following:

a) Note the proposed ICT policies presented within this report;

b) Note the proposed 30 day consultation with staff and the council's recognised trade unions.

c) Note that the proposed policies will be considered by the Cabinet Advisory Group and will also be presented to Cabinet for final approval.

d) Subject to any amendments following consultation with the union, agree the following provision in each of the attached policies: '***any user found to have breached any element of this policy may be subject to disciplinary action, up to and including dismissal'.***

e) Agree that any amendment to the statement referred to at d, above may be approved by the Chief Executive.

3.7 The policies have also been considered by the Cyber Security Cabinet Advisory Group at their inaugural meeting on Tuesday 10 September 2024.

4. Consultation

4.1 Due to the potential disciplinary context of serious breaches of the policies and the subsequent change to an employee's terms and conditions, an all-staff consultation of 30 days was triggered.

4.2 This process was discussed with the council's recognised trade unions, GMB and Unison at the Employee Council meeting on Friday 12 July. At this meeting, the unions agreed to delegate the Chief Executive with the authority to amend the policies as required following the consultation.

4.3 The consultation closed on Monday 2 September. There was no feedback as part of the consultation process. There will be ongoing communications with staff to support the rollout of the four policies to ensure the requirements and implications of non-compliance are understood.

5. Alternative Options

5.1 The alternative is not to approve the proposed updated policies. This is not recommended given the findings identified in para 2.5 of this report.

5.2 It would mean disregarding an agreed management action as part of the EKAP cyber security audit and would also potentially subject the council to an unacceptable level of risk, given that cyber security is one of the council's highest scoring corporate risks at this time.

5.2 As part of this review and approval process, the Cabinet has the opportunity to provide feedback on the proposed policies for consideration and inclusion within the final policies.

6. Corporate Implications

6.1 Finance and Resources

6.1.1 There are no financial implications arising directly from this report or the associated policies/annexes.

6.2 Legal and Constitutional

6.2.1 The use of technology brings significant opportunities but also risks. The Council has legal duties in relation to data security and this requires the Council to consider security at a system and user level. At a system level, security must be designed and implemented at the outset and the Council needs to have robust systems in place to provide resilience in the event of system failure. At a user level it is necessary to create a cyber security culture, ensuring that all staff understand their role to protect the Council's data. The suite of policies being considered will support the Council to protect its data in these regards.

6.2.2 Cabinet should be aware that these policies were considered by the General Purposes Committee and following this were subject to staff and trade union consultation. The requirement to consult staff and trade unions is triggered by a change to an employee's terms and conditions. The Council's current contract of employment requires staff to act in accordance with the Council's Code of Conduct and its policies and regulations including in particular those governing the use of equipment (including protective clothing, computers and software) as well as the use of Council ICT facilities, including email and internet access. The changes proposed in respect of these policies are covered by these provisions. The Council's contract of employment currently also provides the following- 'f*ailure to conform to the Council's rules and regulations may result in disciplinary action against you*.. '. The provisions in relation to disciplinary action set out in this policy are similar to those set out in the Council's standard contract of employment under the section 'Council rules and policies' although in the policies appended to this report, the possibility of dismissal is included. Clearly the result of any disciplinary action may be dismissal however this is not directly referenced in the section referred to above of the Council's standard contract of employment. The results of consultation with both staff and the trade unions are referenced in the relevant section of this report.

6.3 Council Policies and Priorities

6.3.1 These policies sit within the Corporate Priority 5: to work efficiently for you.

The policies are part of the wider digital transformation programme to embed digital technology across council services in reflection of Corporate Priority 5.

6.4 Risk

6.4.1 Cyber security constitutes the highest risk on the Corporate Risk Register at a maximum score of 16 (being risk likelihood x impact). The refreshed policies set out the framework that the council is introducing to reduce that risk in respect of the multiple new processes, measures, and requirements on staff and Councillors to ensure that cyber security is at the forefront of all our digital technology workstreams.

6.4.2 The council has recently introduced a separate Cyber Security Risk Register to gauge and mitigate cyber risk going forward. This was previously included within the wider Digital and ICT Risk Register, but a bespoke plan ensures a more comprehensive risk analysis mechanism as supported by a new internal Security Information Forum which first met in April 2024 and meets monthly.

6.4.3 A dedicated Cyber security Cabinet Advisory Group (CAG) has also been created to provide political oversight of the council's management and mitigations in place in relation to the potential threat posed by cyber attack. The new CAG has also reviewed the council's response to the EKAP audit and the approach taken and ongoing mitigation in place following the January 2024 security incident.

6.5 Climate Change and Biodiversity

6.5.1 There are no clear implications for climate change and biodiversity in respect of this report.

Climate change implications are however included as part of the council's procurement process for new digital or ICT purchases and contracts to ensure that companies/suppliers the council works with give due consideration to climate change factors.

7. Equality, Diversity and Inclusion (EDI) Implications

7.1 An equalities screening tool has been completed and this demonstrates that there are no significant equalities implications arising from the decision sought in this report. The 30 day internal consultation period also provided an opportunity for any EDI considerations to be raised and addressed prior to implementation of the policies.

8. Crime and Disorder Implications and Community impact

8.1 The measures in these policies are designed to reduce both the likelihood and severity of cyber crime affecting the council and our service users. As above, the Cyber Security and Cyber Attacks Policy has been designed in conjunction with the NCSC CAF principles.

9. Subject History

9.1 As per sections 2,3 and 5.

Appendices

Annex 1 - Acceptable Use Policy:
Annex 2 - Cyber Security /Cyber Attacks Policy:
Annex 3 - Digital Security Policy:
Annex 4 - Payment Card Industry Data Security Standards Policy:

Background Papers

Report Author(s) Contact: Hannah Thorpe Head of Strategy and Transformation
telephone: 07879 890923
email: hannah.thorpe@thanet.gov.uk

Report Signed off by
Legal Ingrid Brown (Head of Legal and Democracy & Monitoring Officer)
Finance Matthew Sanham (Head of Finance and Procurement)