Committee and Date	Item
Audit 24 November 2022	Public

Audit Report Management Response – Information Security Management and IT Acceptable Usage Policy

Responsible Officer
e-mail: tim.collard@shropshire.gov.uk Tel: 01743 252756

1. Synopsis

This report outlines the Council's current position and progress made in responding to the Audits for Information Security Management and the IT Acceptable Usage Policy.

2. Executive Summary

2.1. Attached to this report in the Appendix is a Table which provides an update to the various recommendations and management responses made to the two audits referred to with-in the synopsis.

2.2. It is acknowledged that progress is not as advanced as we might have hoped, but there is a plan in place to address all of the outstanding concerns raised within the audits.

2.3. There is currently a system in place for overseeing information governance and security issues. A meeting of the Information Governance/ICT Security Group meets on a monthly basis, chaired by the Assistant Director – Legal and Governance (and Deputy SIRO). In the past six months this meeting has discussed a range of issues including the recent system password changes, cyber security solutions, training and the "phishing tackle test", various policy reviews (eg passwords and removeable media), requests to use external cloud data transfer options such as Dropbox, and the implementation of a data loss prevention process.

2.4. The Council has established the Information Governance Leadership and Organisational Oversight Group of "IGLOO" for short. This is chaired by the Executive Director of Resources (and SIRO) and includes senior officers from across the Council.

2.5. We have commenced the drafting of an Information Governance Framework which will set out in detail the responsibilities of staff, members and various identified statutory roles within the Council. This Policy will then be under-pinned by a wide-range of operational policies such as the Information Security Policy which will set out the standards the Council has put in place to protect information from unauthorised access, use or disclosure.

2.6. The Information Governance Framework will define responsibilities across the organisation. In particular, whilst overall strategic responsibility for information security rests with the Executive Director of Resources as the SIRO and the Assistant Director – Legal and Governance it is envisaged that a more operational day to day oversight will be taken on when an appointment is made to the proposed Head of Governance role.

3. Recommendations

3.1. That Members of the committee consider the progress made on the implementation of the recommendations from the two audit committee reports on Information Security Management and the Acceptable Usage Policy and determine what further measures they would consider to be appropriate.

REPORT

4. Risk Assessment and Opportunities Appraisal

4.1. Information security measures and an effective Acceptable Use Policy are both crucial in mitigating the significant risks the Council faces from cyber attacks.

4.2. Concerns remain about some members and officers who have failed to complete their cyber security training. Various strategies have been introduced to address these concerns which can be discussed with the Committee in more detail.

4.3. A key principle (Principle 6) of the UK GDPR and DPA 2018 is that organisations must process personal data securely by means of appropriate technical and organisational measures. It demonstrates that the council is committed to protecting the data of the citizens it serves. The regular auditing of the Council's Information Governance processes ensure that Principle 6 is complied with.

5. Financial Implications

5.1. The council runs the risk of financial penalties being imposed if personal data breaches occur. If good information governance and

security are in place, the likelihood of breaches occurring will be reduced.

5.2. A successful cyber-attack could mean that the Council's IT systems are locked down unless a substantial fine is paid. Pending resolution of such an attack, the Council would need to revert to alternative mechanisms for delivering its services, all of which are likely to be extremely expensive.

6. Climate Change Appraisal

6.1. There are no direct climate change implications arising from this report.

7. Background

7.1. As can be seen from the table in the Appendix various recommendations have been made as part of the two audits carried out into Information Security Management and the Council's Acceptable Use Policy. Certain of these recommendations are sensitive in nature and if Audit Committee require a more detailed explanation consideration will need to be given to go into Exempt Session.

7.2. In terms of Information Security Management the position is as set out in the Executive Summary. An overarching Information Governance Framework is being developed. Beneath this will be an Information Security Policy (dealing with, amongst other things, the key issue of cyber security). The Framework will be presented to Cabinet for approval probably in January. All other operational procedures, including the Acceptable Use Policy will sit under this over-arching Framework to ensure consistency.

7.3. Data Loss Prevention ("DLP") is the software that can detect and prevent data breaches, exfiltration, or unwanted destruction of sensitive data. Currently Information Governance and ICT Security are discussing how DLP can be implemented and used to provide assurance of correct controls being used to prevent data breaches.

7.4. Another recommendation concerns the need for a record of Information security incidents. Again, there are on-going discussions between Information Governance and ICT Security to establish how current reporting methods can be developed to record all security incidents. This will enable better reporting on all incident types (such as policy breaches, cyber incidents and personal data breaches). Greater clarity on the nature/type of incident will inform what further controls are required to prevent future breaches and quantify the success of any measures put in place.

7.5. In terms of the Acceptable Use Audit, all staff have been reminded about the policy. This has included an explanation of the procedures to follow if there has been a breach of the Acceptable Use policy. Intranet guidance on reporting of information security incidents will be updated when the reporting tool (mentioned in paragraph 7.4) is available.

7.6. A Review of the Mobile and Remote Working Policy is being carried out to reflect new working models. HR and the Communications Teams have been involved in this review.

List of Background Papers (This MUST be completed for all reports, but does not include items containing exempt or confidential information)

Internal Audit Reports:

- Information Security Management 2021/22
- IT Acceptable Usage Policy 2021/22

Cabinet Member (Portfolio Holder)

Rob Gittins

Local Member

All

Appendices

Appendix - Update on Management Responses to Audit Recommendations.