Appendix B – Information Security Framework policies – key features

The following summaries set out the key features of the eight policies outlined in 3.1 of the main report.

B1 Employee Access Policy (covering members as well as staff)

Information Security

- Employees have a responsibility to ensure ICT equipment is suitably located and stored
- Data should not be saved to the local drive of employee devices
- Passwords should be strong, be different to those used for personal purposes and must not be shared, written down or stored where they could be stolen.
- Information stored on electronic and computing devices provided by the Council remains the sole property of the Council
- Employees have a responsibility to promptly report the suspected or actual theft, loss or unauthorized disclosure of Council information
- The Council retains the right to monitor and access use of its data and systems/services to ensure continued compliance with this policy

Email usage

- Council/individual email accounts should be used primarily for business-related purposes
- Employees must not automatically forward email to a third party email system
- The legal status of an email message is similar to any other form of written communication; it should not be considered any less formal than memos or letters
- The Council maintains its legal right, in accordance with current legal and regulatory requirements, to monitor and audit the use of email

Internet/social media usage

- Access to the Internet should only be used for Council/work-related matters
- When using Council resources to access and use the Internet, users must realise they represent the Council
- The Council maintains its legal right, in accordance with current legal and regulatory requirements, to monitor and audit the use of Internet resources
- Employees shall not engage in any Social Media that may harm or tarnish the image, reputation and/or goodwill of the Council and/or any of its employees
- Employees shall not engage in any discriminatory, disparaging, defamatory or harassing comments when using Social Media or otherwise engaging in any conduct prohibited by the Council

B2 ICT Incident Management Policy

- A 'security event' is an adverse event that has caused or has the potential to cause damage to an organisation's assets, reputation and/or personnel
- Security events and weaknesses need to be reported at the earliest possible stage to the ICT Service Desk
- All events that have the potential to result in the unauthorised disclosure of personal or sensitive data must also be reported in accordance with the Data Protection Policy

- Any provided ICT equipment that has been misplaced/lost is to be reported to the ICT Service Desk immediately

B3 NEW Third Party Access Policy

- A risk assessment should be conducted, prior to implementation of any connection, to identify specific requirements
- Any third party organisation with which the Council enters into a connection agreement must be able to demonstrate compliance with the Council's information Security Framework policies
- The Third party must sign a non-disclosure agreement
- Third parties and the Council must inform each other about any security incidents

B4 Removable Media Policy

- Requests for access to – and use of – removable media devices must be made to the ICT Service Desk
- Non-Council owned removable media devices must not be used
- Removable Media should be considered a secondary copy of the data
- All data stored on removable media devices should, where possible be encrypted
- Any misuse or irresponsible actions that affect business data, or any loss of data, should be reported as a security incident to the IT Service desk

B5 Remote Working Policy

- All users must comply with appropriate codes and policies associated with the use of ICT equipment
- All users are expected to undertake a Risk Assessment of their working environment in accordance with Health & Safety policies
- All users are expected to promptly report the theft, loss or unauthorized disclosure of the Organisations information or Equipment
- Any files containing personal data or data which is business critical should be stored on the Organisation's centralised file servers wherever possible and not held on portable computer devices
- No family members may use the IT equipment

B6 NEW Systems Acquisition, Development & Deployment Policy

- All new Information Systems must be formally requested before implementation, through the Council's ICT and Customer Governance Board, and be approved to ensure that they are supportable
- All suppliers engaged with the processing of personal data must complete an Information Sharing Agreement
- Software must only be installed by members of the ICT Service
- Information systems must be secured in an appropriate area, using physical barriers that are commensurate with the identified risks
- Any changes to the systems must be performed in accordance with the Change Management Policy
- All software and licenses must be procured, checked and tested by the ICT Service

B7 NEW Audit and Forensics Policy

The aim of audit and forensics is to provide a systematic, standardised and legal basis for the admissibility of digital evidence that may be required for formal dispute or legal process:

- The logs must be complete, where information is summarised from the logs, it must refer to the original log
- The logs must have appropriate retention rules. Live logs are currently kept for a period of up to one year

B8 NEW Cryptographic Policy

- The current version of laptop encryption is Microsoft BitLocker and Active Directory integrated.
- The standard encryption level is AES 256. A stronger level of encryption may be set for specialist clients but nothing lower.
- Only authorised individuals within the ICT team have access to the recovery key
- No archiving of the keys is to be enacted