Appendix B – Cyber Security

The Council has established a robust framework to manage and mitigate information risk, underpinned by a combination of governance, policy, technical, and procedural controls. The following key assurances are in place:

1. Comprehensive Control Environment

- A layered approach to information risk management is implemented, comprising:
  - **Governance structures**
  - **Policy frameworks**
  - **Technical safeguards**
  - **Awareness and training initiatives**
- These controls collectively ensure that risks are identified, assessed, and mitigated effectively across the organisation.
- The Council follows a “Cloud First” strategy, ensuring systems remain current while implementing additional controls for secure access and usage.
- All technical solutions undergo review by the Technical Design Authority to ensure alignment with strategic goals. A transition to Zero Trust architecture is underway, in line with NCSC guidelines, to address modern threat landscapes. In addition, a business case for infrastructure investment, including security and compliance enhancements, has been approved to support this transition

2. Strategic Oversight and Direction

- Strategic leadership and oversight are provided by:
  - **Information Security Steering Committee (ISSC)**
  - **Strategic Information Governance Group (SIGG)**
  - **Information Governance (IG) Collaboration Group**
- These bodies ensure alignment with organisational goals and regulatory requirements and provide direction for continuous improvement.

3. Policy Framework and Staff Guidance

- A suite of **Information and Data Security policies** is maintained and made accessible via the Centranet.
- Policies are:

    - Regularly reviewed and updated to reflect evolving threats and working practices.
    - Designed to guide staff on secure behaviours and incident response protocols.
- Mandatory e-learning modules on data handling, cyber security, and information assurance are available through the Learning Lounge. In addition, best practice guides are published on the Council's Lighthouse platform and updated regularly.

- Proactive testing is conducted to assess staff understanding, followed by targeted training to improve cyber readiness.

4. Incident Management Assurance

- A **formal Incident Reporting process** is in place and actively communicated to all staff.
- Incidents are:
    - Assessed for impact and root cause.
    - Managed to prevent recurrence and enhance future response capabilities.

5. Compliance with External Standards

- The Council demonstrates compliance with key external standards, including:
    - **Public Services Network (PSN) Code of Connection**
    - **NHS Data Security and Protection Toolkit**
    - **DWP's Memorandum of Understanding (MoU)**
    - **NHS Digital controls**
- Regular **third-party security assessments** are conducted to identify vulnerabilities, with mitigation plans developed and implemented accordingly.