

BROMSGROVE DISTRICT COUNCIL

**Audit, Standards & Governance Committee 15th October
2026**

Cyber Security Assurance and March 2026 Incident Review

Relevant Portfolio Holders	Councillor Simon Nock
Portfolio Holders Consulted	Yes
Relevant Assistant Director	Rob Elmes
Report Author: Peter Bailey	Job Title: ICT Technical Team Leader Contact: p.bailey@bromsgroveandredditch.gov.uk Contact Tel: 01527 881773
Wards Affected	None
Ward Councillor(s) consulted	No
Relevant Council Priority	Risks
Non-Key Decision	
If you have any questions about this report, please contact the report author in advance of the meeting.	
This report contains exempt information as defined in Paragraph 3 of Part I of Schedule 12A to the Local Government Act 1972 (Appendices)	

1. RECOMMENDATIONS

The Committee is asked to RESOLVE that:

- 1) Members are assured of the Council's current cyber security position and the continuing treatment of cyber security as a high corporate risk.**
- 2) Members are assured of the high-level findings from the review of the March 2026 cyber incident, including the effective management of the response and the identified opportunities for improvement.**
- 3) The improvement activity arising from the review be endorsed and that progress will be monitored through the Council's cyber governance arrangements and future Committee updates.**

2. BACKGROUND

- 2.1 Cyber security remains a critical component of the Council's ability to deliver services, protect sensitive information, and maintain public confidence.
- 2.2 This report provides assurance on the Council's current cyber security position, explains how the March 2026 incident tested the Council's arrangements in practice, and sets out the lessons and improvement

Audit, Standards & Governance Committee 15th October 2026

activity arising from the subsequent review. The report also provides an overview of the following:

- The current risk environment and principal mitigations.
- The March 2026 cyber incident and the high-level findings of the external review.
- Ongoing and planned improvements to strengthen resilience.

2.3 Internal audit work has previously identified areas for continued improvement, including cyber awareness, communication, and governance arrangements.

2.4 The Council continues to adopt a risk-based approach, aligning with statutory obligations and recognised good practice.

2.5 The March incident provided a practical test of these arrangements..

3. MARCH 2026 CYBER INCIDENT AND REVIEW

3.1 In March 2026, the Council responded to a cyber incident that required the activation of established incident management arrangements. This report provides members with a proportionate public assurance account.

3.2 The response demonstrated that the Council was well prepared. Established arrangements were mobilised promptly, relevant officers and external partners were coordinated effectively, communications were controlled, and decisions were proportionate to the assessed risk. The incident was contained and remediated with limited disruption to Council services.

3.3 The subsequent external review found that the Council's communications were appropriate in frequency and content, decision-making was aligned to risk appetite, and incident response actions were effective and well-coordinated.

3.4 The principal learning concerned the timing of notifications to external partners. Although communications were appropriate, earlier situational awareness may in some circumstances allow partners to take preventative action sooner. The Council will therefore review notification thresholds while retaining a proportionate approach that avoids unnecessary escalation during periods of uncertainty.

3.5 Actions arising from the review include revising external communication thresholds, enhancing incident response procedures and further

Audit, Standards & Governance Committee 15th October 2026

strengthening partnership working arrangements. Progress will be monitored through the Council's cyber governance arrangements.

- 3.6 Actions arising from the review include revising external communication thresholds, enhancing incident response playbooks and further strengthening partnership working arrangements. The revised thresholds, updated playbooks and partnership arrangements will be reviewed through the Cyber Board during the remainder of 2026/27. Progress will be monitored through the Council's cyber governance arrangements.
- 3.7 The revised report will be considered by the Cyber Board before committee submission. The Board will confirm the appropriate member engagement and reporting route, including alignment with the named lead for the corporate cyber risk and the balance between public assurance and exempt technical detail.

4. OPERATIONAL ISSUES

- 4.1 The Council maintains a layered cyber security approach, combining technical, procedural and organisational controls..

5. FINANCIAL IMPLICATIONS

- 5.1 The March 2026 incident response included engaging with a third party for independent assurance of containment and remediation actions at a cost of £5,500. The response did also require officer time and support from existing suppliers and partners. These indirect costs were absorbed within existing staffing and contractual arrangements and have not been separately quantified.
- 5.2 Current cyber security activity is being managed within approved ICT budgets and existing prioritisation processes. No additional funding requirement is requested through this report.
- 5.3 Further investment may be required as the threat environment and accreditation requirements develop. Any material requirement that cannot be met from existing budgets would be supported by an appropriate business case and considered through the Council's normal budget and governance processes.

6. LEGAL IMPLICATIONS

- 6.1 Cyber security arrangements support compliance with relevant legislation, including:

- Data Protection Act 2018
- UK GDPR
- Computer Misuse Act 1990

6.2 Maintaining appropriate controls reduces the risk of legal and regulatory breaches.

7. OTHER IMPLICATIONS

Local Government Reorganisation

- 7.1 Risks in respect of Local Government Reorganisation include:
- System integration and migration
 - Increased exposure during transition periods
 - Alignment of differing security controls and standards
- 7.2 The ICT service continues to monitor these risks and will support cyber security remaining a core consideration in any transition planning.

Relevant Council Priority

- 7.3 ICT underpins all Council priorities by ensuring:
- Safe and reliable service delivery.
 - Protection of resident and organisational data.
 - Continued operation of critical digital systems.

Climate Change Implications

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

Equalities and Diversity Implications

- 7.5 There are no direct equalities and diversity implications arising from this report.

Community Impact Implications

- 7.6 There are no implications for community safety or health and wellbeing.

8. RISK MANAGEMENT

- 8.1 Cyber security remains a high corporate risk for the Council.

- 8.2 Key risks include:
- Phishing and social engineering attacks

- Data breaches
- Third-party and supply chain vulnerabilities
- Delayed removal of access for leavers.

8.3 Risks are mitigated through:

- Continuous monitoring and threat detection
- Security controls and system hardening
- Staff awareness and training programmes
- Member training – this will form part of the Members' induction and training programme for 2027/28
- Incident response and recovery planning

8.4 Governance and oversight are provided through the Cyber Security Board. The Cyber Security Board provides senior ownership, challenge and oversight on matters requiring wider corporate direction or resources. Cyber risk is also maintained and reviewed through the Council's corporate risk management arrangements, with named ownership, actions and controls monitored in line with the corporate risk framework.

8.5 The March 2026 review reinforced the importance of consistent corporate oversight, clear ownership and disciplined completion of agreed actions. Improvement actions will therefore be assigned to named owners, reviewed regularly by the Cyber Security Board and reported through CLT and corporate risk arrangements where appropriate.

8.6 Member participation in cyber security training is positive, with all but six Bromsgrove Members having completed the most recent Phishing and Cyber Security training. Cyber security training has been classified as mandatory for Members. Optional AI fundamentals training has also been made available to all Members. The small number of outstanding Members have been referred to the Members' ICT Support so that any access issues can be resolved and completion followed up. The position will be reviewed again by December 2026.

9. APPENDICES AND BACKGROUND PAPERS

Appendices

Appendix 1 – Members' KnowBe4 Training Report

Appendix 2 – Cyber Position Statement (EXEMPT)

Appendix 3 – Cyber Attack Response Framework (EXEMPT)

BROMSGROVE DISTRICT COUNCIL

**Audit, Standards & Governance Committee 15th October
2026**

10. REPORT SIGN OFF

Department	Name and Job Title	Date
Portfolio Holder	Councillor Simon Nock	09/10/2026
Financial Services	James Walton, Director of Finance (151)	06/10/2026
Legal Services	Nicola Cummings, Deputy Monitoring Officer and Principal Solicitor - Governance	06/10/2026