Cyber Security Policy

InspirED Pathways

Approved by:	Sharon Cutler	**Date:**	January 2026
Last reviewed on:	January 2026	**Next review due by:**	September 2026

Table of Contents

1. Introduction

Inspired Pathways is committed to safeguarding its information assets, IT systems, and the personal data of students, staff, and stakeholders from cyber threats. This policy sets out our approach to cyber security, outlines roles and responsibilities, and ensures compliance with relevant UK legislation, including the Data Protection Act 2018, UK GDPR, and Keeping Children Safe in Education guidance.

2. Scope

This policy applies to all staff, students, governors, and any third parties who have access to Inspired Pathways' IT systems and data.

3. Roles and Responsibilities

Role	**Responsibilities**
Sharon Cutler, Head of Centre	*Overall responsibility for policy implementation and cyber security strategy.*
Asif Takolia ICT Department (Coventry Council) IT Manager/Team	*Implement technical controls, monitor systems, respond to incidents, manage access and updates.*
Data Protection Officer	Adrian West, DPO Team, Place Directorate, Coventry City Council, Council House Room 57, CV1 5RR
All Staff	Follow this policy, complete annual training, report incidents or concerns promptly within the centre.
Governors	Oversee and review cyber security arrangements and policy compliance.
Students/Users	Use IT systems responsibly and report any concerns.
Nominated Partnership School representatives	Access specific shared pupil file material only.

4. Technical Security Measures

InspirED Pathways in co-ordination with Coventry City Council implements the following security measures, scaled to our size and needs:

- Firewalls and network security controls.
- Anti-virus and anti-malware software on all devices.
- Regular software updates and patch management.
- Secure data backup and tested recovery procedures.
- Encryption for sensitive and personal data.
- Multi-factor authentication (MFA) for critical systems and remote access.
- Secure configuration and monitoring of cloud services (e.g., Office 365, Google Workspace).
- Prompt removal of access for leavers.

5. User Account Management

- Password governance must follow NCSC Guidance:
  - https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/three-random-words
  - https://www.ncsc.gov.uk/collection/passwords/updating-your-approach
- Access control and permissions are based on job roles and reviewed regularly.
- Accounts are promptly disabled when users leave.
- Account activity is monitored and audited.

6. Staff Training and Awareness

- All staff must complete annual cyber security training and annual refresher training.
  - Phishing awareness and social engineering defence training.
  - Corporate Mandatory: Information and Cyber Security (Me Learning)

Practical resources to help schools improve their cyber security: https://www.ncsc.gov.uk/section/education-skills/cyber-security-Centres#section_1**7.**

- Records of cyber training must be retained for all staff and be available for inspection.

7. Incident Response Plan

- All staff members must report any suspected security incidents or concerns to Asif Takolia/Council ICT Department/DPO Team immediately.
  a. Steps for identifying and reporting incidents: Report Incident via Motion / Data Breach - (dpoteam@coventry.gov.uk)
  b. Incident response team: Asif Takolia /Nominated CCC Staff
  c. Communication plan for stakeholders – [e.g. relevant awarding body, National Cyber Security Centre (NCSC), etc.]
  d. Include referral to awarding organisation(s) (if applicable)
  e. Post-incident review process: Conduct a review to identify lessons learned and update procedures if necessary.

8. Compliance and Auditing

- Annual review and update of this policy by Kay Griffin
- Regular internal audits: Annually
- External audits: As deemed

9. Policy Review

- This policy will be reviewed annually by a member of the Senior Leadership Team and updated as necessary to reflect changes in technology, threats, and best practices.
- This policy will be ratified by: [Board of Governors, Senior Leadership Team]

Version	Date of Review	Reviewed By	Next Review Due	Approved By
1	January 2026	Kay Griffin	September 2026	Sharon Cutler