Cyber Security Policy

Date of Approval: 12/09/2025

Signed: Ruth Minhall

Position: CEO and Head of Centre

Next review: 01/09/2026

1. Introduction

Tuition Extra Kent Limited 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 Tuition Extra Kent Limited's IT systems and data.

3. Roles and Responsibilities

Role	Responsibilities
Head of Centre	**Ruth Minhall**, CEO
IT Manager/Team	**Jean-Paul Muller**, Head of Systems and Processes *Implement technical controls, monitor systems, respond to incidents, manage access and updates.*
Data Protection Officer	**Emma Sedgwick,** Designated Safeguarding Lead and Data Protection Officer *Ensure compliance with data protection law, advise on data handling, and oversee data breaches.*
All Staff	*Follow this policy, complete annual training, report incidents or concerns promptly within the centre.*
Governance	*Oversee and review cyber security arrangements and policy compliance.*
Students/Users	*Use IT systems responsibly and report any concerns.*

4. Technical Security Measures

Tuition Extra Kent Limited 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.
- 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 Jean-Paul Muller, Head of Systems and Processes, immediately. Please email jean-paul@tuition-extra.co.uk

a. Steps for identifying and reporting incidents: Any email or issue with any TE device whereby you suspect a cyber security issue may have occurred, must be reported to the Head of Systems and Processes as detailed above.

b. Incident response team: Jean-Paul Muller and our IT Support Supplier.
c. Communication plan for stakeholders JPM to inform CEO
d. 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 – JP Muller
- Regular internal audits: Monthly Security Checks by out IT Support Supplier

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: Ruth Minhall CEO Tuition Extra Group