Cyber Security Policy

Date of Approval: 12/09/2025

Signed: Ruth Minhall

Position: CEO and Head of Centre

Next review: 01/09/2027

Last reviewed: 10 September 2026
Version: 2.0 (Draft for approval)
Policy owner: Jean-Paul Muller, Head of Systems and Processes

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. The Group provides tuition to over 300 children and young people, the majority of whom have Special Educational Needs and Disabilities (SEND), and holds significant volumes of personal, special category and safeguarding data. A successful cyber attack would therefore be a safeguarding incident as well a

1.1 Legal and regulatory framework

This policy is written with regard to the following, and is read alongside them:

- **UK GDPR and the Data Protection Act 2018,** each as amended by the Data (Use and Access) Act 2025 (DUAA), and in particular the Article 5(1)(f) security principle and the Article 32 obligation to implement appropriate technical and organisational measures.
- **Keeping Children Safe in Education (KCSIE),** including the requirement for appropriate filtering and monitoring, which applies to the Group as a provider of education to children.
- **The Department for Education Digital and Technology Standards,** and specifically the cyber security core standard. These standards set out what schools and colleges are expected to have in place, and settings should be working towards meeting them by 2030.
- **The Computer Misuse Act 1990,** which makes unauthorised access to computer material a criminal offence.
- **National Cyber Security Centre (NCSC) guidance,** including its guidance for the education sector and the Cyber Essentials technical controls.

1.2 Position on Cyber Essentials

Cyber Essentials is a government-backed certification covering five technical controls: firewalls, secure configuration, security update management, user access control and malware protection. It is not a legal requirement for an independent provider of our size, and the DfE standards and Cyber Essentials are not the same thing — the DfE standards address governance, process and strategy, while Cyber Essentials assures the technical controls.

The Group has adopted the Cyber Essentials technical controls as its working baseline and will use them as the yardstick for the annual risk

assessment at section 4. Whether to pursue formal certification is a decision for the Executive Board, and is to be reviewed annually, taking into account commissioner and insurer expectations. Staff should note that from April 2026 the scheme treats failure to enable multi-factor authentication on a cloud service that offers it as an automatic failure, which is reflected in section 6 of this policy.

2. Scope

This policy applies to all staff, tutors, contractors, agency workers, volunteers, students, Executive Board members, and any third parties who have access to Tuition Extra Kent Limited's IT systems and data.
It applies across all Group sites, including Roper Road (Canterbury), Maypole Farm and Haven Nook, and to all of the following:

- **All devices** used for Group business — Group-owned laptops, desktops, tablets, mobile phones and servers, and personally owned devices where these are permitted under section 10.
- **All cloud services and systems,** including Microsoft 365, SharePoint, TutorCruncher, MyConcern, finance and HR systems, and any AI tool approved under the AI Governance Framework.
- **All networks,** including Group wired and wireless networks and home or public networks used for remote working.
- **All Group data,** wherever held, including personal, special category, safeguarding, SEND/EHCP, HR and financial data.
- **All suppliers and processors** that host, access or support Group systems or data, including our IT support supplier.

Where a requirement in this policy cannot be met for a specific system or device, the exception must be recorded in the cyber risk assessment with a named owner, a compensating control and a review date.
Undocumented exceptions are not permitted.

3. Roles and Responsibilities

Role	Responsibilities
Head of Centre	**Ruth Minhall**, CEO — Holds ultimate accountability for cyber security. Approves this policy and the annual cyber risk assessment, ensures adequate resourcing, and chairs the response to a major incident.

Role	Responsibilities
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.*
Executive Board	Receives an annual cyber assurance report, approves the risk appetite and the cyber risk assessment, and satisfies itself that cyber risk is being managed. Cyber security is a standing item at least annually.
Designated Safeguarding Lead	**Emma Sedgwick.** Ensures filtering and monitoring meet KCSIE expectations, and leads where a cyber incident has a safeguarding dimension. Holds a veto where a system or configuration presents unacceptable safeguarding risk.
IT Support Supplier	Delivers contracted technical services, monthly security checks and patching, and supports incident response. Performance and security obligations are set out in a written contract reviewed annually under section 11.

Role	Responsibilities
Line Managers / Site Leads	Ensure their teams complete training before being granted access, use only approved systems, and escalate concerns promptly. Notify IT and HR immediately of any leaver or role change.

4. Cyber Risk Assessment and Information Assets

The Group did not previously hold a documented cyber risk assessment. The DfE cyber security standard expects settings to conduct a cyber risk assessment annually and to review it every term, so that the risks attached to hardware, software and data are understood and can be mitigated. The following now applies.

4.1 Risk assessment

- **A cyber risk assessment is completed annually** by the Head of Systems and Processes, with input from the IT support supplier, the DPO and the DSL, and is approved by the Executive Board.
- **It is reviewed every term,** and additionally after any significant incident, any material change to systems, or any significant change in the threat landscape.
- **It assesses the Group against the Cyber Essentials technical controls and the DfE cyber security standard,** identifies gaps, and records for each gap an owner, a mitigation, a target date and a residual risk rating.
- **Material cyber risks are recorded on the Group risk register** and reported to the Executive Board.

4.2 Information asset register

The Group maintains a register of its information assets and digital technology, using the DfE template where suitable. It is owned by the Head of Systems and Processes, held on SharePoint, and reviewed at least termly. It records as a minimum:

- **the hardware in use** — servers, laptops, desktops, tablets, mobile devices and network equipment — with location, owner and support status;
- **the systems and cloud services in use,** their business owner, the categories of data they hold, and whether they hold personal or special category data;

- **the supplier, contract and renewal date** for each system, and whether a written data processing agreement is in place;
- **the end-of-life or end-of-support date** for each item, so that unsupported technology is identified and replaced before it becomes a vulnerability.

Any device or system not recorded on the register is not authorised for use with Group data.

5. 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.

The following requirements give effect to those measures and reflect the Cyber Essentials controls and the DfE cyber security standard.

5.1 Security update management (patching)

- **Critical and high-severity security updates are applied within 14 days of release** to operating systems, browsers, applications and firmware. This timescale is a Cyber Essentials requirement and is monitored by the IT support supplier.
- **Automatic updates are enabled** wherever the platform supports it.
- **Unsupported or end-of-life software and hardware** must be removed from service, or isolated with a documented compensating control and a replacement date recorded in the risk assessment.
- **Evidence of patching** is retained — a patch management or vulnerability dashboard export, rather than self-declaration — and reviewed at the monthly security check.

5.2 Backups and recovery

- **Backups follow the 3-2-1 principle:** at least three copies of data, on two different media, with one copy held offline or immutable and separated from the live environment so that it cannot be encrypted by ransomware.

- **Backups are encrypted,** and access to backup systems requires separate credentials from day-to-day administrative accounts.
- **Restoration is tested at least termly** and the test is documented, including what was restored, how long it took and whether the recovery time objective was met. An untested backup is not a backup.

5.3 Filtering and monitoring

Appropriate filtering and monitoring systems are in place and are reviewed at least annually in line with Keeping Children Safe in Education. Filtering and monitoring is jointly owned by the Head of Systems and Processes and the Designated Safeguarding Lead, and the review confirms that the systems block harmful content without unreasonably restricting teaching and learning. Filtering and monitoring applies equally to AI tools and AI-generated content.

5.4 Email and device security

- **Email authentication** — SPF, DKIM and DMARC — is configured on the tuition-extra.co.uk domain to reduce the risk of spoofing and impersonation.
- **Anti-phishing and anti-spoofing protections** are enabled within Microsoft 365, including external sender warnings and attachment and link scanning.
- **Full-disk encryption** is enabled on all Group laptops, desktops and mobile devices holding Group data.
- **Devices lock automatically** after a period of inactivity and require authentication to unlock.
- **Mobile device management** is applied to Group devices, allowing remote lock and wipe in the event of loss or theft.
- **Secure disposal:** devices and media are securely wiped or physically destroyed before disposal or reuse, and a record of disposal is retained.
- **Logging and monitoring** is enabled on core systems, with alerts for suspicious sign-in activity reviewed by the IT support supplier as part of the monthly security check.

6. 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.
    - **Multi-factor authentication (MFA) is mandatory** on every cloud service that offers it, and on all remote access including VPN and remote desktop. MFA applies to all staff accounts, not only administrative accounts. Where a service offers MFA and it is not enabled, that is a Cyber Essentials automatic failure from April 2026 and must be recorded as an exception in the risk assessment.
    - **Administrative accounts are restricted** to the smallest number of named individuals necessary. Administrators hold a separate admin account for privileged work and use a standard account for everyday tasks such as email and browsing.
    - **Least privilege applies:** accounts are granted the minimum access required for the role, and access to safeguarding, SEND, HR and financial systems is granted only where the role requires it.
    - **Shared or generic accounts are not permitted** except where technically unavoidable, in which case they must be documented, justified and approved by the Head of Systems and Processes.
    - **Joiners, movers and leavers:** access is requested through a documented process, amended promptly on a change of role, and disabled on or before the last working day. HR notifies IT of all leavers and role changes in advance.
    - **Access is formally reviewed at least termly,** including administrative accounts, third-party and supplier accounts, and dormant accounts, which are disabled.
    - **Supplier and third-party accounts** are individually named, time-limited where possible, subject to MFA, and reviewed at each access review.
    - **Passwords** follow the NCSC three random words approach, are never reused between work and personal accounts, and are stored in an approved password manager rather than written down or held in a browser without protection.

7. 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.
    - **Training must be completed at induction,** before access to Group systems and data is granted.
    - **Simulated phishing exercises** are run at least annually. Results inform further training. The exercises are used to educate rather than to penalise, consistent with our no-blame reporting culture.
    - **Role-specific training** is provided to those with administrative privileges, to those handling finance or payroll (given the risk of invoice fraud and impersonation), and to the incident response team.
    - **Executive Board members receive cyber awareness briefing** appropriate to their governance role, so that they can provide effective challenge.

7.1 Student and young person cyber awareness

The DfE cyber security standard expects a cyber awareness plan covering students as well as staff. The Group maintains a proportionate plan for its learners, delivered through PSHE and tutor-led sessions and adapted for the communication and cognitive needs of a SEND cohort. It covers, at an age-appropriate level:

- **keeping accounts and passwords safe** and not sharing logins;
- **recognising phishing, scams and suspicious messages,** including on gaming platforms and social media;
- **what to do and who to tell** if something looks wrong or they think they have made a mistake;
- **the link between online safety and cyber security,** delivered jointly with the Designated Safeguarding Lead and aligned to the Online Safety Policy.

Delivery of the student plan is recorded and reviewed annually alongside this policy.

8. Incident Response

- 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.

8.1 What counts as an incident

A cyber security incident includes, but is not limited to: a suspected or actual phishing click or credential compromise; malware or ransomware; unauthorised access to a system or account; loss or theft of a device; accidental disclosure of personal data; unavailability of a system due to attack; and misuse of Group systems. Staff should report anything that looks wrong. It is always better to report and be wrong than not to report.

8.2 Immediate actions

- **Report first.** Contact the Head of Systems and Processes immediately — jean-paul@tuition-extra.co.uk or by telephone if email may be compromised. Do not delay in order to investigate yourself.
- **Do not attempt to fix or conceal an incident.** Staff will not be penalised for reporting honestly and promptly.
- **Preserve evidence.** Do not delete emails, files or logs. Where a device is suspected of compromise, disconnect it from the network but do not power it off unless instructed, as this can destroy evidence.
- **Containment** is led by the Head of Systems and Processes with the IT support supplier — isolating affected devices, disabling compromised accounts, forcing password resets and revoking sessions.

8.3 Severity and escalation

- **Low** — contained, no data loss, no service disruption. Handled by IT, logged, reported in the monthly summary.
- **Medium** — limited data exposure or localised disruption. Head of Systems and Processes informs the CEO and DPO; DSL informed if a child is affected.
- **High / Critical** — ransomware, significant data loss, or loss of a critical system. The CEO convenes the incident response team; the Executive Board, DPO, DSL and insurers are notified; business continuity arrangements at section 9 are invoked.

8.4 Ransomware

The Group will not pay a ransom. NCSC guidance is clear that payment does not guarantee recovery, does not discharge data protection obligations, and encourages further attacks. Recovery is through the

offline or immutable backups required by section 5.2, which is why the termly restoration test matters. Any ransom demand is reported to the CEO, the police via Action Fraud, and the NCSC.

8.5 External reporting

The DfE cyber security standard requires cyber attacks to be reported. The following reporting duties apply and are the responsibility of the person named against each:

- **Information Commissioner's Office** — where a personal data breach presents a risk to individuals, within 72 hours of becoming aware. DPO decides and reports. Affected individuals are told where the risk is high.
- **Action Fraud** — all cyber crime, including ransomware, fraud and significant phishing. Head of Systems and Processes.
- **National Cyber Security Centre** — significant incidents, via the NCSC reporting route. Head of Systems and Processes.
- **Department for Education** — in line with the DfE expectation that settings report cyber attacks. Head of Systems and Processes, with the CEO.
- **Kent County Council and other commissioners** — where an incident affects the delivery of commissioned provision or the security of data relating to placed children. CEO.
- **Cyber insurers** — promptly, and before engaging any third-party responder, as late notification can invalidate cover. CEO.
- **Police** — by 999 where there is an immediate risk to a child or to life.

8.6 Testing and review

The incident response arrangements are tested at least annually through a tabletop exercise involving the CEO, the Head of Systems and Processes, the DPO, the DSL and the IT support supplier. A ransomware scenario is used at least every other year. Lessons learned are recorded and this policy updated where necessary. A log of all incidents, including near misses, is maintained and reviewed termly.

9. Business Continuity and Disaster Recovery

The DfE standards expect digital technology to be embedded in business continuity and disaster recovery planning. The Group did not previously address this in its cyber policy. The following applies.

- **A business continuity and disaster recovery plan** covering the loss of IT systems is maintained by the Head of Systems and Processes and approved by the Executive Board.

- **Critical systems are identified and prioritised,** with a recovery time objective and recovery point objective agreed for each. Safeguarding systems and the ability to contact families are treated as the highest priority.
- **The plan assumes systems may be unavailable for a prolonged period** and sets out how tuition, safeguarding and communication with families and commissioners continue offline, including paper-based fallback for safeguarding recording.
- **Emergency contact details for staff, key suppliers and the insurer** are held in a form that remains accessible when Group systems are down, including offline.
- **The plan is tested at least annually** alongside the incident response exercise at section 8.6, and reviewed after any significant incident.

10. Suppliers, Remote Working and Personal Devices

10.1 Suppliers and third parties

- **Security is assessed before a supplier is appointed** or a new system adopted, proportionate to the data involved, covering data location, retention, encryption, sub-processors, certifications and breach notification.
- **A written data processing agreement** compliant with Article 28 of the UK GDPR is in place before any supplier processes personal data on our behalf, and a Data Protection Impact Assessment is completed where required.
- **Supplier access is named, time-limited, subject to MFA,** and logged; it is reviewed at each termly access review and revoked promptly at the end of the engagement.
- **Supplier security performance is reviewed annually,** including that of the IT support supplier, and forms part of contract renewal.

10.2 Remote and home working

- **Group data is accessed only through approved systems** and is not stored locally on personal devices or removable media, or in personal cloud storage or personal email.
- **Remote access requires MFA.** Public Wi-Fi is avoided for work involving personal data; where unavoidable, a tethered mobile connection is used in preference.
- **Devices are locked when unattended** and screens positioned so that personal or safeguarding data cannot be overlooked, including at home and when working in a family home during tuition.

10.3 Personal devices (BYOD)

Where a member of staff or tutor accesses Group data on a personal device — including simply reading work email on a personal phone — that device is in scope of this policy and of Cyber Essentials. Such devices must be kept up to date and supported by the manufacturer, be protected by a passcode or biometric lock and by device encryption, have MFA enabled on Group accounts, and must not be shared with family members while Group data is accessible.

Personal devices must not be used to store safeguarding, SEND, HR or financial records, or to photograph students or Group documents. Where a tutor cannot meet these requirements, they must contact the Head of Systems and Processes, who will either arrange a Group-managed device or restrict access. The Executive Board will keep under review whether the Group should move to Group-issued devices only.

10.4 Artificial intelligence

AI tools are in scope of this policy. They must meet the requirements set out here — approved device, supported and up-to-date software, strong authentication and MFA where available — and may only be used in accordance with the Group's AI Governance Framework and AI Acceptable Use Policy. No personal, safeguarding, SEND or HR data may be entered into any AI tool that has not been approved for that purpose by the DPO. Any suspected breach involving an AI tool is reported under section 8.

11. Compliance, Auditing and Assurance

- Annual review and update of this policy – JP Muller
- Regular internal audits: Monthly Security Checks by ou~~t~~r IT Support Supplier
    - The monthly security check covers as a minimum: patch status against the 14-day requirement, backup success and the most recent restoration test, anti-malware status across all devices, MFA coverage, administrative account activity, failed and anomalous sign-ins, and any open vulnerabilities. Findings are recorded and any action is tracked to closure.
    - Termly: review of the cyber risk assessment, the information asset register, user access (including admin and supplier accounts), filtering and monitoring, and the incident log.
    - Annually: full cyber risk assessment, incident response and business continuity exercise, supplier security review, staff and student awareness plan review, and a cyber assurance report to the Executive Board covering incidents, near misses, training completion, audit findings, open risks and progress against the DfE cyber security standard.

- Vulnerability scanning is carried out at a frequency agreed with the IT support supplier, and any critical finding is remediated within 14 days.
- Cyber insurance cover is reviewed annually by the CEO, including the conditions attached to it, so that the Group does not inadvertently breach a policy requirement.
- Breaches of this policy by staff, tutors or contractors are handled under the Group's disciplinary procedures. A serious or deliberate breach may constitute gross misconduct. Unauthorised access to Group systems may also be a criminal offence under the Computer Misuse Act 1990.

12. 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

A review will additionally be triggered by: any significant or repeated cyber incident; a material change to systems, suppliers or sites; a change in legislation, DfE standards, KCSIE or Cyber Essentials requirements; and any finding from an audit, insurer or commissioner.

12.1 Related policies

This policy is read alongside the Data Protection Policy and privacy notices; the Child Protection and Safeguarding Policy and the Online Safety Policy; the CCTV Policy; the AI Governance Framework and AI Acceptable Use Policy; the Acceptable Use of ICT Policy and Staff Code of Conduct; the Business Continuity and Disaster Recovery Plan; and the Group's data breach procedure.

12.2 Outstanding actions

The following are required to give effect to this policy and should be tracked to completion:

- **1.** Complete the first cyber risk assessment and present it to the Executive Board (section 4.1).
- **2.** Compile the information asset register using the DfE template (section 4.2).
- **3.** Audit MFA coverage across all cloud services and remote access, and remediate any gap before April 2026 recertification expectations bite (section 6).

- **4.** Confirm backups meet the 3-2-1 standard with an offline or immutable copy, and run a documented restoration test (section 5.2).
- **5.** Produce the business continuity and disaster recovery plan for loss of IT systems (section 9).
- **6.** Agree and document the student cyber awareness plan with the DSL (section 7.1).
- **7.** Confirm SPF, DKIM and DMARC are correctly configured on the domain (section 5.4).
- **8.** Review the IT support supplier contract against section 10.1 and confirm the Article 28 agreement is in place.
- **9.** Schedule the first tabletop incident exercise (section 8.6).
- **10.** Take an Executive Board decision on whether to pursue Cyber Essentials certification (section 1.2).