KNIGHTSBRIDGE
SCHOOL

Knightsbridge School: Exams Centre Cyber Security Policy 2025-2026

1. Introduction

Knightsbridge School (KS), a member of the Dukes Education Group, is committed to safeguarding its information assets, IT systems, and the personal data of students, including exam candidates from cyber threats. This policy ensures the integrity of the examination process and compliance with the Data Protection Act 2018, UK GDPR, the Data (Use and Access) Act 2025 (DUAA), and JCQ regulations.

2. Scope

This policy applies to all staff (including invigilators), contractors, and any third parties who access KS IT systems, awarding organisation portals (e.g., Pearson, AQA, OCR), or candidate data.

3. Roles and Responsibilities

Role	Responsibilities
Head of Centre	Overall accountability for cyber security strategy and policy implementation.
IT Team	Implementing technical controls, managing firewall/EDR, and ensuring critical patches are applied within 7–14 days.
Data Protection Lead (DPL)	Overseeing data privacy impact assessments (DPIA) for exam software and managing breach notifications to the ICO.
Exams Officer	Managing secure access to awarding body portals and ensuring the confidentiality of electronic question papers.
All Staff	Completing annual mandatory cyber security training and reporting "red flags" immediately.

4. Technical Security Measures

KS employs a multi-layered defence strategy as outlined in the *ICT & Online Safety Policy 2025-26*:

- **Access Control:** Unique user accounts with Multi-Factor Authentication (MFA) are mandatory for all staff accessing exam portals and school email.
- **Endpoint Protection:** All managed, networked devices are equipped with anti-virus and anti-malware capabilities.
- **Patch Management:** We aim to ensure security patches for "critical" vulnerabilities are applied within 14 days of release.
- **Data Encryption:** All candidate data at rest and in transit is encrypted using industry-standard protocols.
- **Secure Backups:** Near continuous secure backups of our main file storage, Google Drive, are stored on the school premises and replicated to a separate, secure off-site location. Daily secure backups of on-site systems are also staged locally with replicas offloaded to a secure off-site cloud storage location.

5. Staff Training and Awareness

- **Annual Training:** All staff engaging with awarding organisation systems must undertake cyber security training annually. Records are maintained by HR and are available for JCQ inspection.
- **Phishing Simulations:** Staff participate in continuous phishing drills to improve "human firewall" resilience.
- **AI Awareness:** Training includes identifying AI-generated phishing attempts (deepfakes) and the risks of "hallucinations" in automated systems.

6. Incident Response Plan

In the event of a suspected cyber incident (e.g., ransomware, unauthorised access to exam papers), KS will follow the *Critical Incident and Emergency Procedures*:

1. **Discovery:** Staff report the incident immediately to the IT Lead and DPL.
2. **Containment:** The IT Team will isolate affected systems but will not power them down (to preserve forensic evidence).
3. **Escalation:** The **Crisis Leader (Gold)** will be notified.
4. **Reporting:** The Exams Officer will notify relevant boards if the integrity of an exam is compromised. The IT Lead / DPL will contact:
    - **NCSC/Action Fraud:** If a significant attack occurs.
    - **ICO:** Within 72 hours if a personal data breach is likely to result in a risk to individuals.

5. **Recovery:** Restoration from secure backups as per the Disaster Recovery plan.

8. Compliance and Auditing

- **Internal Audit:** The school will implement at least annual reviews covering staff cyber-security training, user access controls, device and network security, data protection and encryption, and incident response planning.
- **Policy Review:** This policy will be reviewed annually by the Head of Centre and the Data Privacy Lead to reflect changes in the threat landscape or JCQ requirements.

Authored by: Simon Harrison (Data Privacy Lead) **Date**: 5th September 2025

Reviewed by: Shona Colaço (Head) Date: 10th September 2025

Approved by: Aatif Hassan

Signed: **Date**: 10th September 2025

This policy will be reviewed annually.

(Next scheduled review September 2026)