



GIGGLESWICK SCHOOL

Cyber Security Policy

Lead Author(s)	Chief Operating Officer
Reviewed by	Head of IT
Approval Committee	n.a.
Last review	March 2026
Review frequency	Annual
Next review	March 2027
Policy Type	Statutory

Contents

1	PURPOSE	3
2	SCOPE	3
3	LEGAL AND REGULATORY FRAMEWORK	3
4	GOVERNANCE, ROLES & ACCOUNTABILITY	4
5	POLICY PRINCIPLES AND CONTROL REQUIREMENTS	4
5.1	CYBER HYGIENE & ACCESS CONTROL	4
5.2	FILTERING & MONITORING (SAFEGUARDING)	4
5.3	Exams Security (JCQ)	5
5.4	Data Protection & children’s privacy	5
5.5	Prevent Duty (Online Risk)	5
5.6	Acceptable use & comouter misuse	5
5.7	Third Party & supplier assurance	5
5.8	Backup, continuity & recovery	5
5.9	Training & awareness	6
6.	INCIDENT REPORTING AND RESPONSE	6
7.	RECORDS, EVIDENCE & AUDIT	6
8.	BYOD & REMOTE LEARNING	6
9.	POLICY COMPLIANCE AND ENFORCEMENT	6
10	REVIEW AND CONTINUOUS IMPROVEMENT	6
	APPENDIX A — MINIMUM CONTROL CHECKLIST (EVIDENCE FOR INSPECTION)	6
	APPENDIX B – STAFF AWARENESS QUICK GUIDE (TO BE CIRCULATED)	7
	APPENDIX C – STATUTORY & GUIDANCE SOURCES	7

1 PURPOSE

This policy sets the minimum cyber security, data protection, and online safeguarding requirements for Giggleswick School. It protects learners, staff, and the School's information systems, and ensures compliance with UK law, Department for Education (DfE) statutory guidance (including Keeping Children Safe in Education and the Prevent Duty), and the Joint Council for Qualifications (JCQ) General Regulations and ICE for examinations.

2 SCOPE

This policy covers all School information assets and systems (on-premise and cloud), exam administration systems, endpoints (School-owned and BYOD), networks (including boarding houses), email, collaboration tools, safeguarding/monitoring platforms, and any processing of personal data (including children's data). It applies during term time, out-of-hours activities, trips, exams series, and remote learning.

3 LEGAL AND REGULATORY FRAMEWORK

The School will have regard to and implement controls aligned to the following:

- UK GDPR and Data Protection Act 2018 — lawful processing, security of processing, breach management, rights; ICO education guidance/toolkits.
- Age Appropriate Design Code — children's data: high-privacy defaults, minimisation, profiling/geolocation controls.
- DfE Keeping Children Safe in Education (KCSIE) & Filtering and Monitoring Standard — safe online environment; appropriate filtering & monitoring; annual review.
- Prevent Duty Guidance (latest) — leadership, risk assessment, reducing permissive online environments (e.g., extremist content).
- Education (Independent School Standards) Regulations 2014 — welfare, leadership and management responsibilities.
- Computer Misuse Act 1990 — unauthorised access/acts; tools for cybercrime (School will support investigation/referral).
- NCSC guidance for schools — baseline cyber practices, staff training, governance questions, incident exercises.
- JCQ General Regulations for Approved Centres — cyber security, resilience/contingency, confidentiality; annual cyber training and evidence of completion.
- JCQ ICE (current academic year) — secure handling of examination materials, governance of electronic materials, two-person verification and MFA expectations.

4 GOVERNANCE, ROLES & ACCOUNTABILITY

- Head of Centre (HoC): Overall accountability for compliance with JCQ, KCSIE, Prevent; approves this policy and the annual Cyber & Online Safety Statement to governors.
- Bursar (and Clerk to the Governors): Chairs the Cyber & Data Protection Steering Group; ensures resourcing; oversees supplier risk and insurance.
- Designated Safeguarding Lead (DSL): Leads online safety; collaborates with IT services to ensure effective filtering & monitoring; reports effectiveness to governors annually.
- Exams Officer: Implements JCQ cyber & secure materials controls; maintains logs/evidence; coordinates staff training and contingency arrangements.
- Data Protection Officer (DPO or appointed data lead): Oversees UK GDPR compliance, DPIAs, breaches, SARs, records of processing.
- IT Services (internal/managed): Implements technical controls (MFA, patching, encryption), incident response, backups, and monitoring/reporting.
- All Staff & Pupils: Must follow this policy and report incidents, phishing, or suspicious activity immediately.
- Governors: Provide strategic oversight; review annual filtering/monitoring and cyber posture; challenge assurance.

5 POLICY PRINCIPLES AND CONTROL REQUIREMENTS

5.1 CYBER HYGIENE & ACCESS CONTROL

- Multi-Factor Authentication (MFA): Enforced on all systems holding exam-related data, staff email, MIS/VLE, cloud drives, and awarding body secure sites.
- Passwords: Strong, unique; change exposed passwords; prohibit sharing; secure recovery options set.
- Least Privilege: Role-based access; regular access reviews for staff, invigilators, and contractors.
- Device Hardening: Encryption on all school endpoints; timely security updates; disable unsupported software.

5.2 FILTERING & MONITORING (SAFEGUARDING)

Implement the DfE Filtering & Monitoring standard: assign roles, undertake an annual review, block illegal/inappropriate/harmful content, avoid unreasonable over-blocking; prevent VPN/proxy bypass; extend controls to BYOD as appropriate. DSL and IT collaboratively evidence effectiveness to governors (reports, alerts, trend analysis, incident outcomes).

5.3 EXAMS SECURITY (JCQ)

- **Secure Storage & Handling:** Electronic materials accessed only in secure environment; two-person verification when removing/opening papers; audit logs maintained.
- **Annual Cyber Training:** All staff accessing awarding body systems must complete annual, evidenced cyber training covering passwords, confidentiality, MFA, phishing and reporting. Certificates retained for inspection.
- **Contingency & Resilience:** Plans include impact and response to cyber-attack (e.g., ransomware), alternative site arrangements, and communications with awarding bodies.

5.4 DATA PROTECTION & CHILDREN'S PRIVACY

- **DPIAs for high-risk processing** (new monitoring systems, AI tools, biometrics).
- **Data minimisation and high-privacy defaults** for services used by children; review geolocation/profiling; provide transparent notices in age-appropriate language.
- **Breach Response:** Detect, contain, assess risk; notify ICO and affected parties where required; record breaches and lessons learned.
- **Subject Access Requests & Rights:** Follow ICO guidance, including proportionate search and statutory timelines.

5.5 PREVENT DUTY (ONLINE RISK)

Reduce permissive environments online; block illegal extremist content; train staff to identify, refer, and manage risk; align with Channel referrals and local safeguarding partnerships.

5.6 ACCEPTABLE USE & COMOUTER MISUSE

Prohibit unauthorised access, sharing of credentials, use of hacking tools, or impairment of systems; breaches may lead to disciplinary action and referral under the Computer Misuse Act 1990.

5.7 THIRD PARTY & SUPPLIER ASSURANCE

Conduct due diligence on vendors: security posture, appropriate hosting and data residency, DfE/NCSC-aligned controls, incident SLAs, data processing agreements, and right to audit. Consider Cyber Essentials for relevant suppliers.

5.8 BACKUP, CONTINUITY & RECOVERY

Maintain segregated, immutable backups of critical systems; test restores quarterly; document RTO/RPO targets; include exam timetable and MIS recovery in the Contingency Plan.

5.9 TRAINING & AWARENESS

Provide mandatory annual training for all staff on cyber hygiene and phishing; refreshers for invigilators before each series; targeted modules for DSL, Exams, IT, and governors using NCSC/JCQ materials.

6. INCIDENT REPORTING AND RESPONSE

- Immediate Reporting: Any suspected phishing, malware, data loss, exam material compromise, or filtering bypass must be reported to IT/DSL within one hour.
 - Response Workflow: Triage → Containment → Forensics → Notification (ICO/Police/awarding bodies/parents as applicable) → Recovery → Post-incident review. Use NCSC Exercise in a Box to rehearse scenarios.
 - Exam Incidents: Follow JCQ Suspected Malpractice procedures and notify awarding bodies/JCQ as required.
-

7. RECORDS, EVIDENCE & AUDIT

Maintain evidence logs: access reviews, MFA enforcement, training certificates, filtering & monitoring reports, exam secure handling logs, incident registers, DPIAs, supplier due diligence, and annual assurance to governors/ISI.

8. BYOD & REMOTE LEARNING

BYOD permitted only where devices meet School security baseline (updated OS, device encryption, screen lock, no jailbreaking; School MDM/profile when accessing School systems). Filtering & monitoring should apply in line with the DfE standard.

9. POLICY COMPLIANCE AND ENFORCEMENT

Non-compliance may result in disciplinary action and/or revocation of access; in cases of unauthorised access or impairment, the School may involve law enforcement under the Computer Misuse Act 1990.

10 REVIEW AND CONTINUOUS IMPROVEMENT

This policy will be reviewed annually (or earlier following incidents or changes in DfE/JCQ/ICO guidance). The review will include: (i) cyber risk assessment; (ii) filtering & monitoring annual effectiveness review; (iii) staff training coverage; (iv) exam season readiness checks; (v) Prevent online risk assessment updates.

APPENDIX A – MINIMUM CONTROL CHECKLIST (EVIDENCE FOR INSPECTION)

- MFA enabled on: MIS, Email, VLE, awarding body portals, exam data shares. (Screenshots/policy export)
- Annual cyber training certificates for all staff with access to awarding body systems; invigilator briefings prior to each series. (Training log + certificates)
- Secure handling logs for exam materials (electronic & physical); two-person verification records.
- Filtering & Monitoring Annual Review (roles, SEND/EAL considerations, AI/GenAI risks, BYOD coverage, illegal URL enforcement, VPN/proxy controls). (Board report)
- DPIAs for high-risk tech (monitoring tools, AI, biometrics); high-privacy defaults documented.
- Backups tested quarterly; immutable/segregated storage; recovery runbook.
- Incident Response rehearsal (NCSC Exercise in a Box) and post-incident reviews.
- Prevent Duty online risk controls & referral pathway documented; staff training records.

APPENDIX B – STAFF AWARENESS QUICK GUIDE (TO BE CIRCULATED)

- Think before you click — verify sender; report phishing using School process.
- Use MFA — never share one-time codes; secure recovery options.
- Handle exam materials securely — only in secure rooms; no personal devices; follow ICE.
- Children’s privacy first — minimise data; avoid sharing; check age-appropriate defaults.
- Report concerns — extremist/illegal content or online harm: inform DSL promptly (Prevent Duty applies).

APPENDIX C – STATUTORY & GUIDANCE SOURCES

- DfE Keeping Children Safe in Education (current): <https://www.gov.uk/government/publications/keeping-children-safe-in-education>
- DfE Filtering & Monitoring Standard: <https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges/filtering-and-monitoring-core-standard>
- ICO Data Protection in Schools guidance: <https://www.gov.uk/guidance/data-protection-in-schools>
- ICO Age Appropriate Design Code: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/>

- Prevent Duty Guidance (England & Wales):
<https://www.gov.uk/government/publications/prevent-duty-guidance>
- Education (Independent School Standards) Regulations 2014:
<https://www.legislation.gov.uk/uksi/2014/3283>
- Computer Misuse Act 1990: <https://www.legislation.gov.uk/ukpga/1990/18/contents>
- NCSC Cyber Security for Schools: <https://www.ncsc.gov.uk/section/education-skills/cyber-security-schools>
- JCQ General Regulations for Approved Centres: <https://www.jcq.org.uk/exams-office/general-regulations/>
- JCQ ICE — Instructions for Conducting Examinations:
<https://www.jcq.org.uk/exams-office/ice--instructions-for-conducting-examinations/>

Branding placeholders: Once the School provides the official crest/logo and colour palette, the header and heading colour styles can be updated accordingly. The Table of Contents will populate after opening in Word and updating fields (select the TOC and press F9).