ST DOMINIC'S GRAMMAR SCHOOL

ONLINE SAFETY, ACCEPTABLE USE AND DATA SECURITY POLICY

Academic Year 2026–2027

Safeguarding priority. Data protection law does not prevent necessary and proportionate information sharing to protect a child. Immediate risk must be reported to the DSL without delay.

Policy control	Approved position
Applies to	Whole School: Nursery and EYFS to Sixth Form; staff, governors, volunteers, contractors and relevant visitors
Policy owner	Headmaster
Operational lead	DSL Mrs Nikki Hastings-Smith; Data Protection Lead Sharon Tillett; Network Manager Mr B James
Proprietor	Mr Gary Hartland
Approval date	30 August 2026
Effective date	1 September 2026
Next review	By 31 August 2027, or earlier following material legal, regulatory, safeguarding or technological change
Publication	Staff SharePoint; relevant public information on the School website

Quick reporting routes

Concern	Report immediately to	First response
Child at risk, harmful content, grooming, sexual imagery or cyberbullying	DSL or Deputy DSL	Safeguarding procedure; support the child; preserve evidence safely; do not investigate independently.
Filtering or monitoring alert	DSL and Network Manager	DSL makes safeguarding decisions; IT provides technical containment and evidence.
Misdirected email, lost device, unauthorised access or disclosure	Sharon Tillett stillett@sdgschool.co.uk and Network Manager Brian James bnjames@sdgschool.co.uk	Contain and record immediately; assess safeguarding and breach risk.
Malware, compromised account or unavailable systems	Network Manager and Headmaster; DSL if pupils may be affected	Isolate or contain; activate continuity arrangements; retain logs.
Concern about staff conduct online	Headmaster/DSL through allegations or low-level-concerns procedure	Do not confront or investigate independently.
Concern involving the Headmaster	Proprietor and DSL as appropriate	Use the safeguarding and allegations procedures.

1. Purpose and scope

This policy establishes the School's whole-school arrangements for online safety, filtering and monitoring, cyber and information security, acceptable use and the safe handling of personal information through technology. It applies whenever School accounts, data, networks, devices or services are used, and to off-site online conduct that affects safeguarding, welfare, discipline or the lawful operation of the School.

The standalone Data Protection and UK GDPR Policy governs the School's full data-protection framework. This policy restates the immediate requirements users need when working online; it does not replace the standalone policy, privacy notices, Records Retention Schedule, breach procedure or rights-request procedure.

2. Legal and regulatory framework

- Education (Independent School Standards) Regulations 2014 and current DfE guidance on the Standards.
- Keeping Children Safe in Education 2026; Working Together to Safeguard Children 2026; Prevent duty guidance; EYFS statutory framework.
- UK GDPR; Data Protection Act 2018; Data (Use and Access) Act 2025; Privacy and Electronic Communications Regulations 2003.
- Computer Misuse Act 1990; Copyright, Designs and Patents Act 1988; Online Safety Act 2023 and relevant communications, sexual-offence and image-abuse legislation.
- DfE filtering and monitoring, cyber security, mobile phone, EdTech and generative-AI guidance; current ISI framework and handbook.

3. Core principles

- Online safety is a safeguarding responsibility, not solely an IT function.

- Safeguarding decisions are made by the DSL; technical staff support but do not determine safeguarding outcomes.
- Controls are proportionate to age, vulnerability, SEND, EAL, curriculum need and context.
- Access to monitoring data is restricted to authorised, trained personnel.
- Personal information is processed lawfully, minimally, accurately, securely and only for approved purposes.
- Users can report accidental access or mistakes without fear of being blamed for seeking help.
- The School records risk assessments, checks, incidents, decisions, reviews and completion of actions.

4. Roles and accountability

Role	Responsibilities
Proprietor/Governing Body	Approve and challenge; receive annual assurance on safeguarding, filtering, monitoring, cyber security, incidents, training and action closure.
Headmaster/SLT	Resource and enforce the policy; approve systems and exceptions; coordinate serious incidents and continuity.
DSL	Lead online safety; triage alerts; identify vulnerability; support/referral; review trends and effectiveness.
Network Manager	Configure, test and document controls; manage authorised access; preserve logs; contain incidents; report to DSL/SLT.
Data Protection Lead	Advise on lawful handling, DPIAs, breaches, procurement, rights and training; maintain records and escalate material risk.
Staff	Supervise pupils; use approved systems; protect information; report concerns, errors and near misses immediately.
Pupils	Follow the AUP; protect accounts and privacy; report harm, suspicious activity or accidental access.
Parents/carers	Support expectations and reporting; avoid publishing information or images about other children without a proper basis.

5. Online risk and education

The School addresses the KCSIE categories of content, contact, conduct and commerce, including illegal and sexual content, self-harm, suicide and eating-disorder material, hate and extremism, misinformation, grooming, coercion, sextortion, cyberbullying, harassment, intimate-image abuse, scams, gambling, doxxing, impersonation, deepfakes, cloned voices, fake screenshots, algorithmic targeting and excessive use.

- Online-safety education is embedded across computing, PSHE/RSHE, assemblies and the wider curriculum and is revisited by age and risk.
- EYFS pupils learn simple rules about trusted adults, permission, privacy, kindness and reporting worrying screen content.
- Pupils learn source evaluation, consent, privacy, copyright, scams, manipulative design, AI limitations and reporting.
- Staff receive induction and refreshers covering KCSIE, filtering/monitoring, phishing, secure sharing, breaches, AI and reporting routes.
- Parents receive accessible updates on emerging risks, mobile phones, home controls and reporting.

6. Filtering and monitoring

Sophos is the School's approved filtering and monitoring product. Its configuration, coverage and limitations must be verified and documented rather than assumed. Filtering should block illegal and harmful content

without unreasonably restricting teaching and learning, including on School-managed devices off site where technically possible.

- The DSL and Network Manager record the responsible SLT and governance links, absence cover and escalation thresholds.
- Checks are undertaken and recorded at a frequency determined by risk; changes, outages, new services or incidents trigger additional checks.
- The DSL reviews relevant reports and alerts promptly. No alert is treated as proof of wrongdoing.
- Block/allow decisions record requester, educational purpose, risks, decision, approver, duration and review date.
- The annual review considers age, SEND/EAL, vulnerable pupils, Prevent, BYOD, AI, encrypted traffic, circumvention and technical limitations.
- Authorised monitoring data is accessed only by trained staff, retained according to a documented schedule and linked to safeguarding procedures.

7. Accounts, devices and remote access

- Use named accounts, strong unique passwords and multi-factor authentication where provided; never share credentials.
- Lock screens, apply updates and use encryption and approved storage. Privileged accounts are separately controlled.
- Personal hotspots, VPNs, proxy services, tethering and attempts to bypass controls are prohibited.
- BYOD requires express approval, appropriate security and the ability to remove School data.
- School information must not be copied to personal email, consumer cloud storage, unapproved removable media or public AI tools.
- Personal messaging or social-media accounts must not be used to communicate with pupils except under a formally approved and recorded emergency arrangement.
- Lost devices, suspicious logins, phishing, malware, misdirection and near misses must be reported immediately.

8. Mobile phones, images and communications

The School maintains its approved mobile-phone expectations, with recorded reasonable adjustments for medical need, disability/SEND, safeguarding or another exceptional reason. Devices and evidence are handled under current searching, screening, safeguarding and behaviour procedures.

- Official communications use approved accounts. Check recipients, attachments, links, permissions and sensitivity before sending.
- Photographs, audio and video require a legitimate School purpose and approved device/process; use minimum identifying information.
- Staff maintain professional boundaries and do not form personal online connections with current pupils.
- Live streaming, biometrics or facial recognition require senior approval, a lawful basis, necessity/proportionality assessment and DPIA.
- Parents and visitors must not publish identifiable information about other children where this creates privacy or safeguarding risk.

9. Generative AI and emerging technology

- Only School-approved tools may be used for School business or with pupils; age limits, terms, data use, location, security, accessibility, bias and monitoring compatibility are assessed first.
- Do not enter pupil, safeguarding, SEND, medical, HR, assessment or other confidential information into a public or unapproved AI service.

- Approved personal-data use requires a lawful basis, transparency, processor terms, retention/training-use review, transfer safeguards, human oversight and DPIA screening.
- AI output is unverified and must be checked for accuracy, bias, fabrication, copyright and appropriateness.
- Material AI use is described in privacy information. Significant automated decisions receive the safeguards required by law.
- Sexualised, degrading, deceptive or impersonating AI content about a person is prohibited and may be a safeguarding or criminal matter.

10. Personal data and secure handling

Required standard. Collect and access only what is necessary; use it only for the approved purpose; keep it accurate; share only through approved secure methods; retain it according to the Records Retention Schedule; and dispose of it securely.

- Access is role-based, reviewed and removed promptly when no longer required.
- Records must be factual, necessary, professional and appropriately separated from opinion.
- Safeguarding information is shared when necessary and proportionate; fear of GDPR must never delay protection of a child.
- New apps, cloud services, plugins and suppliers require authorised procurement, Article 28 terms where applicable, security checks and DPIA screening before use.
- Rights requests, complaints and requests for correction must be forwarded immediately to Sharon Tillett, regardless of wording.

11. Responding to online-safety and cyber incidents

1. Make safe: attend to immediate danger or distress; contact emergency services where necessary; report to the DSL.
2. Preserve: do not forward illegal or sexual material; record a factual account, URLs/usernames and times; follow DSL/police guidance.
3. Triage: the DSL considers safeguarding, child-on-child abuse, criminality, Prevent, mental health, SEND, parents and referral.
4. Contain: IT restricts accounts/content or isolates equipment under DSL/SLT direction while preserving evidence and continuity.
5. Record and act: use safeguarding, behaviour, cyber and data records; support those affected; make proportionate decisions after context is considered.
6. Follow up: check wellbeing and retaliation, review controls and curriculum, identify trends, assign actions and verify completion.

12. Personal data breaches

A personal data breach includes accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data. It includes near misses that could reveal control weaknesses.

Time	Required action
Immediately	Tell Sharon Tillett and the Network Manager; recall or restrict access where possible; do not conceal the error or delete evidence.
Contain	Restrict access, reset credentials, preserve logs and maintain essential safeguarding and continuity arrangements.
Assess	Record the nature, people and data affected, likely consequences and safeguards; DSL assesses any child risk.

Time	Required action
Within 72 hours of awareness	The Data Protection Lead advises the Headmaster/Proprietor on ICO notification where risk to rights and freedoms is likely; reasons are recorded if not notified.
Without undue delay	Inform affected individuals where high risk is likely unless a lawful exception applies; give practical protective advice.
Afterwards	Record decisions and learning; review suppliers, controls, training and governance assurance.

13. Review and assurance

At least annually, leaders report to the Proprietor/Governing Body on the online-safety risk assessment; filtering/monitoring review; cyber controls and recovery tests; incidents and trends; vulnerable pupils; pupil/parent/staff voice; curriculum; AUP compliance; training; breaches; processor/EdTech risks; and completion of actions. Effectiveness is judged through evidence, not merely low incident numbers.

Appendix 1 – Staff, governors, volunteers and contractors AUP

By using School systems or signing the annual declaration, I agree that I will:

- use technology lawfully, professionally and only for authorised purposes;
- use my named account, protect credentials, use MFA where provided and lock the screen;
- use approved email, storage, messaging, devices, platforms and AI tools;
- check recipients, attachments, permissions and sensitivity and use secure transfer;
- maintain professional boundaries and never communicate privately with pupils through personal services;
- supervise pupils actively and report concerning content, disclosures, alerts or bypass attempts;
- not bypass controls, install unapproved software, access another user's information or make unauthorised recordings;
- use personal devices for School data only where authorised and secured;
- report loss, misdirection, disclosure, phishing, malware, account compromise and near misses immediately;
- understand that proportionate monitoring may occur and misuse may lead to safeguarding, disciplinary, contractual or legal action.

Name: _____ Role: _____

Signature: _____ Date: _____

Appendix 2 – Pupil AUP: Reception and Prep

- I ask a trusted adult before using a new app, website, game or device.
- I keep passwords and personal information private, except when a trusted adult needs to help.
- I am kind and do not take or share someone's picture, voice or work without permission.
- If I see something worrying, confusing or unkind, I stop and tell an adult. I will not be blamed for asking for help.
- I use only the accounts, devices and sites my teacher has allowed and do not try to avoid safety controls.
- I know trained adults may check School activity to help keep everyone safe.

Pupil: _____ Class: _____ Date: _____

Parent/carer acknowledgement: _____ Date: _____

Appendix 3 – Pupil AUP: Senior School and Sixth Form

- use School technology for learning and authorised activities and follow mobile-phone and examination rules;
- protect my account, use strong passwords/MFA, lock devices and report compromise;
- respect privacy, consent, copyright and dignity and not bully, impersonate, dox or create deceptive/deepfake material;
- not seek, create or distribute illegal, harmful, intimate or discriminatory content; if encountered accidentally, stop and report without forwarding;
- not use a VPN, proxy, hotspot, tethering, another account or technical trick to bypass controls;
- use only approved AI tools, disclose AI help when required, verify outputs and never enter another person's confidential information;
- not take, publish or livestream images/audio/video without permission and a legitimate purpose;
- tell a trusted adult about harmful content, coercion, grooming, scams, security problems or behaviour affecting anyone;

- understand School systems are monitored proportionately and serious misuse may be addressed through safeguarding, behaviour or legal procedures.

Pupil: _____ Year: _____ Date: _____

Pupil signature: _____ Parent/carer: _____

Appendix 4 – Authoritative sources

- Keeping Children Safe in Education 2026.
- DfE data protection in schools guidance, updated 9 July 2026.
- DfE filtering and monitoring and cyber security standards.
- DfE guidance on generative AI, EdTech procurement and data protection.
- ICO UK GDPR, children's information, security, breach and accountability guidance.
- Independent School Standards guidance and current ISI framework and handbook.