Online Safety Policy

Hollygirt School
NOTTINGHAM

Date of Review:	08/01/2026 / Version 1.0
Policy Review Led by:	Headteacher
Approval by Trustees:	02/02/2026
Date of Next Review:	January 2027

Table of Contents

To be read in conjunction with the following polices

- All Adults Code of Conduct
- Anti-Bullying & Cyberbullying Policy
- Behaviour & Discipline Policy
- Critical Incident Management and Disaster Recovery Policy
- Cyber Security Policy
- Data Protection Policy
- Exams Policy
- Non-Examined Assessment (NEA) Policy
- Safeguarding & Child Protection Policy
- Staff Code of Conduct
- Taking, Storing and Using Images of Children Policy

This policy will be reviewed annually.

1. Statement of Intent

The internet and connected technologies are integral to teaching, learning and daily life. This policy sets out how the school will provide a safe, secure and age-appropriate digital environment, educate pupils and staff to use technology responsibly, and respond proportionately to online safety concerns. The aims are to:

- Safeguard and protect all members of the school community online.
- Embed online safety as a core element of safeguarding and pastoral care, and prepare pupils for life beyond school.
- Define roles, responsibilities and procedures that enable safe, lawful and ethical use of technology.

2. Scope

This policy applies on site, off site (e.g., trips), and online (including guided home learning/remote education). It covers school-owned and personal devices, school networks and cloud platforms, and behaviour that occurs off-site but impacts the school (e.g., cyberbullying). It applies across the whole school.

3. Roles and Responsibilities

3.1. Trustees & Senior Leadership

Provide strategic oversight and ensure online safety is embedded across safeguarding, curriculum and IT systems; receive regular reports and ensure statutory compliance (e.g., KCSIE, Prevent).

3.2. Headteacher

Has overall responsibility for online safety provision, resources, training and escalation pathways.

3.3. Designated Safeguarding Lead (DSL)

Leads day-to-day online safety: maintains procedures, curates training/resources, oversees filtering/monitoring alerts, and coordinates responses and referrals.

3.4. Technical Staff/ IT Team

Implement secure, age-appropriate filtering and active monitoring; maintain systems security (e.g., anti-virus, authentication, auditing) and support investigations.

3.5. Data Protection Lead

Acts as the person responsible for data protection; advises on lawful processing, third-party due diligence, breach handling and staff training. Staff must notify the Data Protection Lead of suspected and/or actual personal data breaches without delay.

3.6. Examinations Officer and SENDCo (Access Arrangements)

Ensure exam systems (including mock exams) are conducted in line with JCQ and awarding-body rules; manage access arrangements and special consideration; secure papers, scripts and NEA materials; and train invigilators. These roles work with IT to secure digital materials, restrict access to candidate work, and maintain back-ups.

3.7. All Staff

Model safe, professional practice; supervise pupils; embed digital citizenship; follow reporting procedures; and uphold data protection and information security requirements. Staff must follow the **All Adults Code of Conduct** for online contact, social media, ICT use and use of images.

3.8. Pupils

Engage in age-appropriate learning; follow Acceptable Use Agreements (AUAs); respect others; and report concerns to a trusted adult.

3.9. Parents/Carers

Support online safety at home, discuss school expectations with their children, model appropriate use, and seek help where concerned.

4. Education and Training

4.1. Curriculum (EYFS – KS4)

Online safety is taught through Computing, PSHE/RSE, Form activities, and cross-curricular activities, with messages reinforced whenever technology is used. Teaching and instruction include: safe search and research; critical evaluation of online information; respectful communication; privacy and data; copyright and academic honesty; recognising scams/misinformation; and resilience to radicalisation. Provision is differentiated for vulnerable learners (e.g., SEND) and is age appropriate.

4.2. Staff

Induction covers Safeguarding, All Adults Code of Conduct and Staff AUA. Annual updates and periodic INSET sessions address emerging risks (e.g., scams, social media trends, AI) and statutory changes. Staff are reminded that school systems are monitored and online conduct (in/out of school) must remain professional.

4.3. Parents/Carers

The school provides guidance via talks, newsletters and signposting of website content; highlights the platforms pupils use and expected behaviours; and encourages use of home filtering/safe-search.

5. Acceptable Use & Behaviour

5.1. AUAs

Separate AUAs exist for pupils and for staff. AUAs state permitted uses, privacy expectations, academic integrity, and reporting routes; they must be read and signed annually (parents co-sign for younger pupils). **See Pupil AUA; Staff AUA**.

5.2. Conduct

Members of the community must not access, create, store or share illegal, harmful or inappropriate content (e.g., pornography; hate; extremist material), must not bully or harass, and must respect privacy and copyright. Cyberbullying concerns will be managed in line with the Anti-Bullying & Cyberbullying Policy, including timelines for response, support and sanctions. **See All Adults Code of Conduct**.

5.3. Social Media & Contact with Pupils

Staff must keep communications within professional boundaries, use school systems, and must not share personal contact details or engage with pupils via personal social media. Any online friendship/contact risks must be reported to the DSL. **See All Adults Code of Conduct.**

5.4. Academic Integrity & NEA/Exams

Pupils must follow JCQ rules for NEA and exams, including authenticity of work, appropriate referencing, and not sharing assessed work online or via social media; inappropriate use of AI in assessments constitutes malpractice. **See Exams Policy; Exams Malpractice Policy.**

6. Safer Technology Environment

6.1. Devices and Platforms

School provides/permits age-appropriate access to computers and **Microsoft 365** services (including Teams, OneDrive, SharePoint, and Outlook) as the primary platform for learning and collaboration. Staff must check any online websites, tools, and apps, including any browser add-ons and AI LLMs, for suitability and data compliance with the IT technician before allowing pupils to access.

6.2. Filtering and Monitoring

The school implements proportionate filtering and active monitoring aligned to statutory requirements (KCSIE; Prevent). The school complies with the DfE 'Filtering and Monitoring Standards' and the DSL reviews the logs for safeguarding triggers. Systems:

- block illegal/harmful content (e.g., CSAM; extremism);
- generate timely alerts for DSL investigation;
- apply age-appropriate rules; and
- are regularly audited and updated.

6.3. Network and Security

All users authenticate with individual credentials; anti-virus and patches are maintained; guest Wi-Fi is segregated; activity is logged; and removable media use is restricted. The school reserves the right to monitor, intercept and review use of school IT with appropriate and proportional reason and intent; staff should have no expectation of privacy on school systems.

6.4. Data Protection and Information Security

The school processes personal data in line with the UK GDPR principles (lawfulness, fairness/transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity/confidentiality; accountability). Staff must:

- handle data lawfully and securely; keep accurate records; and store only as long as necessary;
- report suspected/actual personal data breaches to the Data Protection Lead immediately—serious breaches may need ICO notification within 72 hours;
- complete due-diligence for new third-party platforms via the Bursar before use;
- not remove personal data from site without the consent of the Headteacher or Bursar consent; any authorised off-site storage must be encrypted;
- avoid using non-approved/personal platforms for pupil data, including but not limited to Generative AI models.

6.5. Mobile Phones

The School operates a phone pouch system so phones are locked away and unusable during the school day unless for academic purposes directed by the class teacher; in Prep, any phones brought for travel are held by Form Teachers until the end of the day. Confiscation and searches follow government guidance and the school's Search Policy. **See Behaviour and Discipline policy.**

6.6. Images and Recording

Images of pupils are captured, stored and shared only in accordance with consent records and the Taking, Storing and Using Images of Children Policy. Staff must use only school-provided/authorised equipment, avoid one-to-one photography, and follow guidance on naming and publishing images (e.g., first names only, group images

where possible). Personal devices must not be used for pupil images. **See Taking, Storing and Using Images of Children Policy**.

6.7. Microsoft 356 Security Measures (what the school enforces)

- **Encryption**: Microsoft 365 encrypts data at rest and in transit; only supported protocols are permitted for client connections.
- **Identity & Access**: Multifactor authentication (MFA) is required for all staff and administrators for offsite access.
- **Threat Protection** (email, Teams, SharePoint/OneDrive): Microsoft defender is installed and monitored on all windows devices. Alerts are notified on the BCX Network Management Tool and monitored. On-premises hardware firewall running WatchGuard with active Gateway Antivirus, Intrusion Prevention Service and Botnet Detection. Annual online training is mandatory for all staff on Online safety and UK Data protection – courses available will be monitored and updated on a regular basis to ensure staff's knowledge and skills are maintained.
- **Information Protection & DLP**: SharePoint admin centre policies in place regarding sharing and access control. Redstor cloud backups used for all data, mailboxes and active on-site servers. Further details for incident management can be found in the Critical Incident Management and Disaster Recovery Policy.
- **External Sharing Controls**: OneDrive/SharePoint default to Specific people links; external guests must verify identity. Default link expiry and view-only / block-download are encouraged for sensitive content; domain restrictions are used where appropriate.
- **Data Lifecycle**: OneDrive/SharePoint is used for all school data, Data retention for deleted users is currently set for 1 year. Regular checks and reviews of backups are in place to maintain compliance.

6.8. Use of Artificial Intelligence (AI)

AI is becoming increasingly prevalent in everyday technology; it offers many positive opportunities for improving staff wellbeing by reducing workload but also comes with many inherent risks including, but not limited to data breaches, plagiarism, and safeguarding risks.

The school believes developments in technology should be embraced positively. We aim to support both pupils and staff in becoming confident users of AI to support learning and productivity, whilst ensuring all are aware of common pitfalls and more serious risks which could compromise an individual's safety or data. Staff are trained via INSET sessions and continuing professional development.

To mitigate against risk, the following principles must be followed:

- Each member of staff has an individual responsibility to protect pupil, parent, and colleague data and intellectual property.
- Data and Intellectual Property (IP) **must not** be entered into a Large Language Model (LLM) or other Generative AI model which uses input for learning.
- Only approved LLMs may be used to generate materials using any data or IP. In both cases, these can only be used when logged in via a Hollygirt account:
    - Microsoft Copilot
    - The National College

- Staff should not share login details and/or allow others to use their Hollygirt accounts to access and use LLMs.
- Pupils must not be directed to use LLM or other AI tools outside of the classroom eg: for homework.
- When utilising LLMs or other AI tools in the classroom, staff must ensure there is explicit instruction to pupils regarding risks and safe usage.
- Staff must remain aware that individuals under the age of 13 are not permitted to have accounts with LLMs or other AI tools and must not set work in class that requires a login. For pupils 13+, a Hollygirt login must be used to access, only, the approved LLMs and AI tools.
- Each member of staff has an individual responsibility to be familiar with the suite of examination policies and the individual requirements of the examinations boards they follow to ensure that any AI use in the construction of examined materials meets regulations, including appropriate referencing.

6.9. NEA Digital Security and Exams Materials

IT and curriculum staff must restrict access to candidates' NEA work between sessions; maintain effective back-ups (including off-site); and consider encryption of sensitive media. Examinations staff secure digital/paper materials (question papers, scripts) and follow JCQ storage/dispatch rules. **See Non-Examined Assessment Policy.**

7. Responding to Online Safety Incidents

7.1. Reporting and Recording

Concerns (e.g., cyberbullying; sharing of nudes/semi-nudes; harmful content; breaches of filtering; suspected exam/NEA malpractice involving online behaviour or AI) are reported immediately to the DSL and recorded on CPOMS, and/or the Assistant Head Academic as appropriate. The school will acknowledge a report and conduct a proportionate investigation, inform parents of those involved, and identify support/sanctions as required. **See Safeguarding and Child Protection Policy; Anti-Bullying and Cyberbullying Policy; Behaviour and Discipline Policy; Exams Malpractice Policy.**

7.2. Searching, Screening and Confiscation

Searches are conducted lawfully and proportionately; devices may be examined where there is good reason; indecent images of children must never be intentionally viewed. Devices are secured and referred to DSL/police as appropriate. Where criminal offences are suspected (e.g., malicious communications/harassment), the school will inform the police. **See Safeguarding and Child Protection Policy**.

7.3. Exams & NEA Malpractice (online)

Suspected misuse of AI, plagiarism, sharing assessed work, or breaches of JCQ rules are escalated to the Examinations Officer, Head of Department and DSL, and handled in line with the Exams/NEA/Malpractice procedures. **See Exam Malpractice Policy.**

7.4. Data Breaches

Any breach involving personal data is escalated per the Data Protection Policy. The ICO will be notified within 72 hours if there is a serious breach of personal data.

Action Fraud will be notified for all significant cybercrimes. Serious incidents will be reported to the DfE sector.incidentreporting@education.gov.uk. **See Data Protection Policy.**

A hard copy of the Incident Response Plan is kept in a physical location (in case the network is encrypted)

8. Education Phases and Age Specific Expectations

The below offer a summary of, but are not limited to, key principles for each phase.

8.1. EYFS/KS1 (Ages 3 – 7)

- Adult-supervised use only; simple, visual rules; focus on asking for help, being kind, and keeping personal information private.
- AUA is explained by adults and co-signed by parents.

8.2. KS2 (Ages 7 – 11)

- Teach safe searching, evaluating information, respectful messaging, and basic copyright/plagiarism; introduce risks of anonymous platforms; reinforce reporting.

8.3. KS3/KS4 (Ages 11 – 16)

- Emphasise digital footprint, social media privacy, academic honesty, scams/phishing, radicalisation resilience, and legal frameworks (e.g., Computer Misuse Act; Communications Act; Protection of Children Act).

9. Remote Education / Guided Home Learning

Remote learning is delivered via Microsoft 365 tools, primarily Teams and OneDrive. Sessions may be recorded for safeguarding; access is restricted; visiting speakers are vetted and supervised; parents are advised to use home filtering/safe-search. Staff and pupils follow conduct protocols (e.g., appropriate dress/background; no personal recordings). **See Remote Education Plan**.

10. Practical Guidance for Microsoft Teams and OneDrive (for staff and pupils)

10.1. Microsoft Teams Etiquette

- Join on time; test audio/video and use appropriate backgrounds; keep microphones **muted when not speaking**.
- Use **Raise hand**, chat and reactions to participate without talking over others; appoint a moderator for larger meetings/classes.
- Use the **lobby** to control admission; do not post meeting links publicly; only record with a clear educational purpose and inform participants.
- Keep discussions in the correct **channels**; use @mentions responsibly; follow school behaviour standards in chat and meetings.

- Use only school accounts/systems for contact with pupils; do not share personal numbers, email or social media.

10.2. OneDrive/SharePoint file-sharing

- Prefer **Specific people** links with expiry; avoid "Anyone with the link" except for approved public materials.
- For sensitive content, use **view-only** and **block download**; store school-owned documents in SharePoint/Teams rather than personal OneDrive.
- Remove access when collaboration ends; review permissions and link reports regularly.

10.3. Exams/NEA – practical online safety reminders for candidates

- Do **not** share assessed work (drafts or final) online or via social media; keep all NEA materials secure and private.
- Reference sources appropriately; maintain records of research/planning; do not plagiarise or use AI to generate content beyond permitted guidance.
- Follow invigilator and examinations staff instructions regarding devices and identification on exam days.

Appendix A: Microsoft 365 Best Practices for Safeguarding (summary)

1. **Identity & Access**
    a. Enforce MFA for staff, administrators and other high-risk roles; enable for pupils where appropriate.
    b. Use Conditional Access: block legacy authentication; require MFA for risky/ sign-ins/off-site access; restrict to compliant or hybrid-joined devices; define trusted locations; exclude only emergency accounts.

2. **Threat Protection**
    a. Turn on Defender for Office 365 preset security policies; enable Safe Links across email, Office apps and Teams; enable Safe Attachments for email and for SharePoint/OneDrive/Teams.

3. **Information Protection & DLP**
    a. Implement sensitivity labels with a simple classification scheme (e.g., Public / Internal / Confidential / Restricted) and auto-labelling where feasible; require encryption for restricted content; enable DLP policies to prevent external sharing of sensitive data.

4. **External Collaboration**
    a. Default to Specific people links; require guest identity verification; enforce link expiry; use domain allow/deny lists where appropriate; consider guest access expiration.

5. **Data Lifecycle & Audit**
    a. Apply retention policies and labels to Exchange, SharePoint, OneDrive and Teams; review periodically; monitor audit logs and alerts.

Appendix B: Pupil IT Acceptable Use Agreement

When using devices, websites, apps, I will:

Be Safe

- Keep my passwords private.
- Never share personal details online.
- Tell a teacher if something online makes me worried or uncomfortable.
-

Be Respectful

- Use technology for learning only.
- Be polite in messages and posts.
- Not bully, harass, or share hurtful content; including via social media at any time.

Be Responsible

- Not try to access blocked sites or change settings.
- Not download or share illegal or inappropriate material.
- Not use AI tools unless my teacher says it's allowed.

Protect Work & Privacy

- Save work in my school account (e.g., Teams/OneDrive).
- Not share my work or exams online.
- Not take or share photos/videos of others without permission.

Report Problems

- If I see something wrong, unsafe, or upsetting online, I will tell a teacher straight away.

I understand that breaking these rules may mean losing access to school systems and other consequences.

Name:	
Form:	
Signature:	
Date:	

Appendix C: Staff IT Acceptable Use Agreement

Staff IT Acceptable Use Agreement

Applies to: all adults working for or on behalf of the school (employees, trustees, trainees, contractors, volunteers).

Covers: school-owned and personal devices when used for school business; school networks and cloud platforms (e.g., Microsoft 365: Teams, OneDrive, SharePoint, Outlook); on-site, off-site and remote/online activity.

1) Professional use & boundaries

- Use IT systems solely for legitimate school purposes and in line with professional standards and safeguarding duties.
- Do not share personal contact details or use personal social media to communicate with pupils. Use school platforms only.
- Keep communications transparent, respectful and recordable; avoid any content that could be misinterpreted.

2) Safeguarding online

- Never access, create, store or share illegal, harmful or inappropriate content (e.g., pornography, hate/extremist material, indecent images). Report any accidental exposure immediately to the DSL.
- Challenge and report cyberbullying, harassment or unsafe online behaviour affecting pupils or staff.
- Follow procedures for searching, screening and confiscation; never intentionally view indecent images of children. Escalate concerns to DSL.

3) Data protection & information security

- Process personal data lawfully, minimally and securely. Store only for as long as necessary and on approved systems.
- Report data breaches immediately to the Data Protection Lead; do not attempt to delete, conceal or investigate independently.
- Do not email or share sensitive data externally without appropriate access controls (e.g., sensitivity labels, 'specific people' links, block-download).
- Personal devices: ensure passcode/MFA-protections are enabled; check you are logged into school accounts before sharing/sending any files or data; ensure any downloads to personal devices are deleted once actioned and never store pupil or parent data outside approved apps.

4) Accounts and passwords.

- Keep credentials confidential and unique. Do not share logins or allow others to use your account.
- You are responsible for all actions taken using your account—report any suspicious sign-in alerts or compromise immediately.

5) Email, messaging & file sharing (Microsoft 365)

- Use school email/Teams for school business. Maintain a professional tone; avoid unmoderated group chats with pupils.

- When sharing files: prefer SharePoint/Teams over personal OneDrive; use 'Specific people' links with expiry; apply sensitivity labels where required.
- Do not publish meeting links publicly; recordings only where educationally necessary and with notice to participants.

6) Mobile phones, images & recordings
- Follow school procedures on mobile phone use; pupils' phones remain secured unless teacher-directed for learning.
- Images of pupils: use only school-approved equipment; follow consent records; never use personal devices.

7) Use of AI tools
- Do not input pupil, parent, colleague personal data or school IP into AI tools that learn from prompts. Use only approved AI solutions via school accounts (e.g., Microsoft Copilot; The National College) and follow examination rules and referencing requirements when using AI in lessons.
- Do not direct pupils to use LLMs at home; in class, provide explicit safety guidance and adhere to age restrictions.

8) Monitoring & privacy
- The school monitors use of IT systems (email, internet, Teams, file storage) for security and compliance. Staff should have no expectation of total privacy on school systems; the school will apply proportionate and appropriate monitoring.
- CCTV operates on site and may be used as evidence in investigations.

9) Security & safe tech use
- Do not install unauthorised software on school devices, add-ins or connect unapproved hardware/removable media.
- Be alert to phishing and suspicious links/attachments; report and delete; Defender 'Safe Links/Safe Attachments' are in place but not foolproof.
- Conduct due diligence with the Bursar/IT before using any third-party platforms with pupil data or sites which require pupils to create an account.

10) Remote education & off-site work
- Use Microsoft 365 (Teams/OneDrive) for remote learning; keep backgrounds appropriate; no personal recordings.
- Do not remove personal data off-site (outside of Hollygirt Network and authorised apps/cloud based services) without Headteacher approval, or Bursar approval in the absence of the Headteacher; ensure encryption and secure storage if authorised.

11) Exams/NEA integrity
- Follow JCQ/awarding-body rules; maintain authenticity; apply proper referencing; no inappropriate AI use; never share assessed work online.

12) Reporting concerns
- Immediately report safeguarding, online safety, malpractice, or data concerns to the Dat Protection Lead/DSL/Head as appropriate and record on CPOMS if required.
- Report low-level concerns and any incidents that might be misconstrued; cooperate with investigations.

Proportionate sanctions: Breaches may lead to restricted access, disciplinary action up to and including dismissal, referral to external agencies where required, and/or police involvement for illegal content.

Please sign the declaration and return to the Bursar.

Staff IT Acceptable Use Agreement

Name:	
Role:	
Signature:	
Date:	