Link Governor: SM
Date of last review: 15 November 2026

# ONLINE SAFETY POLICY

**Table of Contents**


| | |
|---|---|
| **1.** | **Policy Scope** |
| **2.** | **Policy Development, Monitoring and Review** |
| **3.** | **Acceptable Use** |
| **4.** | **Leadership & Responsibilities** |
| **5.** | **Reporting, Responding, Recording and Monitoring** *Includes Flowchart for Dealing with Online Safety Incidents* |
| **6.** | **Use of Artificial Intelligence (AI)** |
| **7.** | **Education** |
| **8.** | **Technology** |
| **9.** | **Filtering and Monitoring** |
| **10.** | **Technical Security** |
| **11.** | **Cyber Security** |
| **12.** | **Data Protection** |
| **13.** | **Technology Practice** |
| **14.** | **Device Management** |
| **15.** | **Digital Content** |
| **16.** | **Public Online Communications** |
| **17.** | **Outcomes** |
| **Appendix A** | **KCS Acceptable Use Agreements (AUAs)** |
| **Appendix B** | **Kingdom Christian School Acceptable/Unacceptable Use tables** |
| **Appendix C** | **Flowchart: Decision-making for dealing with online safety incidents.** |
| **Appendix D** | **AI Risk Assessment Matrix Template** |
| **Appendix E** | **Responding to Learner Actions table** |
| **Appendix F** | **Responding to Staff Actions table** |

This policy applies to all members of the school community (including staff, learners, volunteers, parents and carers, visitors, community users) who have access to and are users of school digital systems, both in and out of the school. It also applies to the use of personal digital technology on the school site (where allowed).

## 1. Policy Scope

This Online Safety Policy sets out how Kingdom Christian School will safeguard members of our community online, in line with statutory guidance and best practice**.** The school is aware of the wider statutory requirements that informs this policy.

This policy applies to all members of the school community who access or use school digital systems, including staff, learners, governors, volunteers, parents/carers, visitors and community users**.** It applies to use of school systems both on and off site**,** and to the use of personal devices on the school site (where permitted). It is shared with staff during induction and through training, communicated to learners and parents/carers through Acceptable Use Agreements (AUAs) and awareness activity and is published on the school website.

Where online safety concerns or incidents occur outside school and are known to the school, Kingdom Christian School will respond in line with this policy and related procedures, including the school's Safeguarding, Behaviour and Anti**-**Bullying policies. Where appropriate, parents/carers will be informed of incidents involving inappropriate online behaviour that take place out of school.

## 2. Policy Development, Monitoring and Review

The Online Safety Policy is part of the school safeguarding framework and should be read alongside the following policies:

- **Safeguarding Policy**
- **Behaviour Policy**
- **Anti-Bullying Policy**
- **Data Protection Policy**

The policy:

- Defines responsibilities for online safety.

- Sets expectations for safe, professional and ethical use of technology (including AI).
- Sets out reporting, recording and response procedures for online safety incidents.
- Supports compliance with KCSIE, DfE Technical Standards and UK GDPR.
- Promotes learners' digital competence and critical understanding.

This policy is maintained by Mark Ozenbrook, Headteacher and DSL, with the deputy DSLs and Safeguarding and Online Safety Governor, drawing on school staff and relevant technical support.

Mark Ozenbrook is the responsible senior leader for filtering and monitoring. The DSL and Safeguarding and Online Safety Governor monitor this policy. Online safety assurance is reported at each governing body meeting, with a formal effectiveness review at least once every academic year.

| |
|---|
| Mark Ozenbrook - Headteacher, designated safeguarding lead (DSL), responsible senior leader for filtering and monitoring, and Google Admin Console administrator for pupil accounts.<br>Rebecca Jennings - Deputy Headteacher and deputy DSL.<br>Shani Ozenbrook - Headteacher and deputy DSL.<br>Lorraine Pooley - School Business Manager and authorised Senso user; escalates safeguarding concerns to the DSL or a deputy.<br>Stephanie McCubbin (Steph) - Safeguarding and Online Safety Governor; receives anonymised assurance reports and challenges effectiveness.<br>James Gill, Switch Voice and Data - School firewall administrator; coordinates firewall and network checks with Mark Ozenbrook.<br>Nathan Welsh, Bloobo IT Support - Microsoft account administrator; implements school-authorised Microsoft account and service settings. |

The school will evaluate the effectiveness of this policy using evidence such as:

- Logs of reported online safety incidents
- Filtering and monitoring records
- Internal network activity monitoring data
- Surveys/questionnaires of: Learners, Parents/carers, Staff

This policy supports the school's statutory safeguarding duties. It is reviewed by the governing body at least annually, or sooner following significant technological developments, emerging risks or incidents.

## 3. Acceptable Use

Acceptable use is defined through the **Online Safety Policy** and a suite of Acceptable Use Agreements (AUAs*).* We understand that AUAs matter most when they are understood, reinforced and followed—not simply signed.

We use the following AUAs which are included in Appendix A of this policy.

- Learner KS2 AUA
- Staff and Volunteer AUA
- Parent/Carer AUA

Our AUAs are reinforced to our school community in the following ways:

- staff and learner induction/handbooks
- posters in areas where technology is used
- curriculum and awareness sessions
- communications with parents/carers
- school website
- peer support / learner-led activity

Information of acceptable/unacceptable use at Kingdom Christian School is recorded in the tables in **Appendix B** of this policy.
For school-approved enterprise lessons, pupils may prepare descriptions, item photographs and costings offline and discuss them as a class. An authorised adult operates any marketplace account, publishes listings and handles buyers, payments and returns. Pupils do not access the account, contact buyers or disclose personal details. The school approves the account and financial arrangements; applicable platform age and seller rules still apply.

## 4. Leadership & Responsibilities

Online safety is a shared responsibility. All members of the school community are expected to model safe, responsible behaviour, report concerns promptly and learn from incidents and good practice. The roles below clarify accountability.

### ❖ Headteacher & Senior Leaders

Senior leaders set the culture and ensure that systems are effective. In line with KCSIE, the DSL holds day-to-day lead responsibility.

Senior leaders will:

- Ensure the school meets its safeguarding duty of care, including online safety.
- Follow the Safeguarding and Allegations policies for concerns about adults. Concerns about a Headteacher go to the chair of governors or proprietor, not to the subject of the concern.

- Ensure that the DSL and relevant colleagues are trained and able to fulfil their roles.
- Put in place appropriate oversight and support for internal monitoring activity.
- Establish and receive regular online safety reports and act on emerging risks and themes.
- Work with governors, the DSL and IT provider on filtering and monitoring.

❖ **Governors**

Governors approve the Online Safety Policy and challenge its effectiveness, in line with KCSIE expectations.

The nominated Safeguarding and Online Safety Governor is Stephanie McCubbin (Steph), who will:

- Meet regularly with the DSL
- Receive anonymised incident and monitoring summaries.
- Check delivery of key commitments (e.g., education, reporting, staff training).
- Through regular review, assess the effectiveness of filtering and monitoring with SLT, DSL and IT provider, in line with DfE standards.
- Undertake basic cyber security awareness training and support school cyber security oversight.
- Governors also support parent/carer and community engagement in online safety.

❖ **Designated Safeguarding Lead (DSL)**

KCSIE states the DSL leads safeguarding and child protection, including online safety, and understands filtering and monitoring systems and processes.

The DSL will:

- Lead safeguarding, including online safety, with clear responsibilities in their job description.
- Maintain up-to-date knowledge of online risks, filtering/monitoring and cyber security.
- Coordinate and record online safety concerns and incidents, escalating and referring in line with safeguarding procedures.
- Liaise with SLT, the Online Safety Governor, the IT provider and relevant external partners as required.
- Review filtering and monitoring trends, oversee weekly Monday checks and arrange the recorded annual effectiveness review and checks following changes or incidents.

- Report regularly to SLT and drive continuous improvement across relevant policies and practice, using evidence (e.g. incident data, monitoring, self-review)
- Ensure appropriate support for learners with SEND.

### ❖ Curriculum Leads

Curriculum leads will work with the DSL to deliver a planned online safety programme through appropriate channels, e.g. Computing, PSHE/RSE, other curriculum areas, assemblies/pastoral provision and national initiatives e.g. Safer Internet Day.

### ❖ Teaching and Support Staff

All staff are expected to uphold professional standards online and contribute to a strong safeguarding culture.

Staff will:

- Follow the **Online Safety Policy**, **Safeguarding Policy**, **Technical Security Policy** and sign/comply with the **Staff Code of Conduct**.
- Maintain professional boundaries (including online/remote learning).
- Supervise learner use of technology and follow procedures for online safety issues
- Embed online safety where appropriate; teach research skills, copyright and plagiarism awareness.
- Challenge harmful online behaviour and report concerns promptly.
- Use only school-approved digital services and AI tools; protect data, apply UK GDPR, and verify AI outputs for accuracy/bias before use.
- Complete induction and annual training, with updates as needed; contribute to improvement by sharing learning and concerns.

### ❖ IT service provider

Senso console access is restricted to Mark Ozenbrook, Shani Ozenbrook, Rebecca Jennings and Lorraine Pooley. All four have received online safety and other appropriate training. They use individual authorised accounts and access only information needed for their role. Governors and external IT contacts are not granted Senso console access by this policy.

The IT provider supports leaders and the DSL to meet DfE filtering, monitoring and technical standards. Where services are outsourced, the school remains accountable.
James Gill at Switch Voice and Data manages the school firewall. Nathan Welsh at Bloobo IT Support manages Microsoft accounts. Mark Ozenbrook manages

pupil accounts through Google Admin Console. External technical support acts on school-authorised instructions; the school retains safeguarding accountability.

The IT provider will:

- Maintain secure infrastructure and managed user access.
- Implement approved technical changes within the provider's remit and supply evidence of checks to Mark Ozenbrook. Senso console access remains restricted to the four authorised school users.
- Support procurement, risk identification, reviews and checks with SLT/DSL.
- Report technical weaknesses or safeguarding concerns promptly to Mark Ozenbrook or a deputy DSL; do not make safeguarding judgements on the school's behalf.
- Follow the school's Online Safety and **Technical Security policies** and keep technical knowledge current.

### ❖ Learners

Learners will:

- Follow the **Online Safety Policy** (including personal devices where permitted).
- Report concerns and know how to get help.
- Use technology responsibly, respecting others and their copyright and intellectual property.
- Participate in teacher-operated AI demonstrations or use only the specifically approved iLearn2 AI activity, with staff supervision. Never access staff AI accounts or unapproved AI.
- Understand that out-of-school behaviour may be addressed where it affects the school community.

### ❖ Parents and carers

Parents/carers are key partners in reinforcing safe online behaviour.

The school will:

- Publish the **Online Safety Policy**
- Provide guidance on the responsible use of online technologies and seek permissions for digital services/images where required.
- Share updates through meetings, newsletters, online channels and campaigns.

Parents/carers will be encouraged to reinforce key messages and support safe use of personal devices (where permitted in school).

## 5. Reporting, Responding, Recording and Monitoring

The school is committed to creating a culture where all members of the community feel confident, safe, and supported in reporting online safety concerns. In line with Keeping Children Safe in Education (KCSIE, 2026), the school recognises that online risks may occur in school or outside school and may affect children in any setting. Reporting routes must therefore be clear, accessible, inclusive, and consistently understood by all.

The school recognises national findings, including the Ofsted Review of Sexual Abuse in Schools and Colleges (2021), which highlight that children may not always feel able to report. The school assumes that harmful online behaviours may be occurring, even where none have been disclosed, and responds by maintaining strong systems for reporting, analysing, and addressing concerns.

### Reporting Concerns

Report online safety or AI safeguarding concerns immediately to Mark Ozenbrook, Headteacher and DSL. If he is unavailable, contact Rebecca Jennings, Deputy Headteacher and deputy DSL, or Shani Ozenbrook, Headteacher and deputy DSL. Do not wait for the weekly review. Concerns about a Headteacher follow the separate allegations/whistleblowing route to the chair of governors or proprietor, with LADO advice as appropriate. Immediate danger requires emergency services. Data breaches also follow the Data Protection Policy and its DPO/adviser reporting route.

The school will ensure that:

- Clear, accessible reporting routes are in place for all members of the school community, including pupils, staff, governors, parents/carers, and volunteers.
- Reporting processes are fully aligned with safeguarding procedures, including the **Safeguarding Policy**, **Whistleblowing Policy**, **Allegations of Abuse Policy** and **Complaints Policy**.
- Multiple reporting options are available, such as speaking with the Designated Safeguarding Lead (DSL), online or anonymous reporting tools, email contact, or in-person disclosures.
- Reporting routes are well publicised through induction, assemblies, posters, the school website, and digital platforms.

- All users understand that any online safety concern must be reported, including those relating to harmful or illegal behaviour, sexual harassment, bullying, discrimination, grooming, or self-generated sexual imagery.

**Responding to Concerns**

The school will ensure that:

- Reports are acknowledged and responded to promptly, considering the safety and wellbeing of the person reporting.
- The DSL, Online Safety Lead, and senior leaders have the training and skills needed to recognise, assess, and manage online safety risks.
- Where a report indicates possible illegal activity or serious harm, it is escalated immediately through safeguarding procedures. Examples include (but are not limited to):
  - Child sexual abuse material (CSAM)
  - Non-consensual or self-generated images
  - Grooming, exploitation, or sexual harassment
  - Terrorism or extremism
  - Hate crime, fraud, extortion, stalking
  - Cyber offences under the Computer Misuse Act
  - Sale of illegal substances or goods
- Where concerns do not involve suspected illegal activity, devices may be checked using a safe, controlled, and documented process involving senior staff and a designated review device.
- AI-supported monitoring systems, where used, are subject to human oversight to ensure contextual understanding.
- Users who report concerns receive reassurance, appropriate support, and feedback on the outcome.

**Recording and Monitoring**

The school will:

- Maintain a secure and confidential record of all incidents, including actions, decisions, and follow-up.
- Ensure reports are audited and analysed regularly to identify emerging trends, patterns of concern, and the effectiveness of responses.
- Provide anonymised summaries of trends and learning to:
  - Governors (via safeguarding reports)

- *Staff*
- *Learners, where appropriate*
- *Parents/carers through general communications*
- *Local safeguarding partners where relevant*

**External Support and Escalation**

The school will work with appropriate external agencies when required, including:

- Local Authority safeguarding teams
- Local Authority Designated Officer (LADO)
- Police / CEOP
- Local Safeguarding Partnership guidance (e.g., harmful sexual behaviour support)
- *UK Safer Internet Centre's Professionals Online Safety Helpline*
- *Reporting Harmful Content service*

See **Appendix C** for the flowchart Decision-making for dealing with online safety incidents.

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures as follows:

See Appendix E for Responding to Learner Actions and Appendix F for Responding to Staff Actions. Safeguarding assessment takes priority; the tables do not impose automatic sanctions.

## 6. Use of Artificial Intelligence (AI)

Teachers may demonstrate school-approved AI from the front of the classroom and take questions from pupils. The teacher operates the account, enters prompts and checks responses before displaying or using them. Pupils must not operate a staff account. Direct pupil AI use is permitted only for school-approved, age-appropriate activities through the school subscription to iLearn2

(ilearn2.co.uk), with staff supervision and the approved services enabled through Senso.

Microsoft Copilot is approved for authorised staff use and teacher-operated demonstrations, subject to the recorded account and service settings. Pupils aged 3-11 must not use Copilot directly: Microsoft excludes under-13s from Copilot Chat. Staff use school-managed Microsoft accounts; Nathan Welsh at Bloobo IT Support manages those accounts on the school's instructions.

**AI approval and Senso access**

Only school-approved AI may be accessed through the Senso whitelist (allow list) on all school computers. Approval records must distinguish staff demonstrations from direct pupil use and identify the exact service, feature, URL, age/year group, purpose, permitted inputs and review date. A whitelist entry does not approve every feature or make a tool suitable for every child. New or externally linked tools within iLearn2 need their own checks before access is enabled.

Mark Ozenbrook approves the educational and safeguarding use after consultation with the deputies and the school's data protection adviser/DPO where needed. An authorised Senso user implements the recorded whitelist change. Mark coordinates any firewall change with James Gill and Microsoft settings with Nathan Welsh. The relevant staff and pupil profiles must be tested on all school computers before use, including new or replacement computers. Staff-only approval must not open a service to pupil accounts.

The school subscription to iLearn2 provides the approved route for direct pupil AI learning. Staff select activities suitable for the pupils' actual age, development and SEND needs. An educational subscription is not blanket approval for every linked website, app or AI feature. Pupils do not create personal AI accounts or use unrestricted public chatbots.

**Safe use, privacy and educational integrity**

Do not enter identifiable pupil information, photographs, videos, SEND, medical, safeguarding or behaviour records into generative AI prompts or uploads. Initials and codes do not make identifiable information anonymous. Approved iLearn2 activities may use task responses and non-identifying prompts within the recorded limits; there is no blanket permission to upload pupil work. A proposed educational workflow involving non-identifying pupil work, voice or account data requires specific approval and data protection assessment before use. Approval or whitelisting does not override the prohibited inputs above; any proposed exception requires a prior policy review. Pupil material must not be used to train AI models.

Staff must verify outputs for accuracy, bias and appropriateness and retain responsibility for teaching, assessment and decisions. AI may support general feedback strategies; individual pupil work and assessment records are not uploaded unless a separately approved workflow expressly permits this. Where AI materially supports an output, staff explain that assistance where appropriate. Copyright and confidentiality requirements remain applicable.

The approved-tool record must consider provider terms, age limits, account settings, data collection and retention, model-training use, linked services and technical limitations. The school completes a DPIA where required before processing. Parent and pupil information explains the actual use and monitoring. Whitelisting alone is not evidence of lawful data processing.

**Reporting and review**

Report online safety or AI safeguarding concerns immediately to Mark Ozenbrook, Headteacher and DSL. If he is unavailable, contact Rebecca Jennings, Deputy Headteacher and deputy DSL, or Shani Ozenbrook, Headteacher and deputy DSL. Do not wait for the weekly review. Concerns about a Headteacher follow the separate allegations/whistleblowing route to the chair of governors or proprietor, with LADO advice as appropriate. Immediate danger requires emergency services. Data breaches also follow the Data Protection Policy and its DPO/adviser reporting route.

The Generative AI Policy sets out the detailed approval process and authorised-use record. Use Appendix D for each AI risk assessment, supported by the 2026 online safety audit and action plan. Review an activity when the tool, links, features, age group, data use or risks change. Do not mark checks complete without the supporting evidence.

Misuse is addressed through safeguarding and the relevant behaviour or staff procedures. Children reporting a concern are supported; an accidental exposure or request for help is not automatically a disciplinary matter.

## 7. Education

Online safety education is a core part of the school's safeguarding approach and sits alongside effective technical controls (including filtering and monitoring). In line with KCSIE, online safety is a running and interrelated theme reflected across relevant policies and the curriculum.

The school delivers a planned, progressive and inclusive programme of online safety education for all learners, aligned to nationally recognised guidance and frameworks (including DfE "Teaching Online Safety in Schools", UKCIS "Education

for a Connected World"). Learning is age-appropriate, builds on prior learning, is matched to need, and is taught through existing curriculum areas (including RSHE/RSE, computing) with assessment and clear intended outcomes.

The programme develops learners' ability to:

- recognise and manage online risks, including harmful content, contact, conduct and commerce risks;
- understand consent, supported by safe opportunities for discussion;
- think critically about what they see online, including how to check reliability and accuracy and the role of AI-generated content;
- respect copyright and intellectual property, including when using online material and AI tools;
- understand and follow the learner acceptable use agreement, and act within moral and legal boundaries (including awareness of the Computer Misuse Act 1990).

Staff guide and supervise planned internet use. Any filtering exception requires recorded approval by Mark Ozenbrook and implementation by an authorised user. Exceptions must not disable illegal-content protections, circumvent age restrictions or allow unapproved AI. Curriculum need alone does not authorise a teacher to change Senso settings.

Learner voice is actively used to strengthen the school's approach through feedback, learner representation

**Education - Staff**

In line with DfE Keeping Children Safe in Education (KCSIE, 2026), all staff and volunteers receive safeguarding and child protection training, including online safety, at induction and through regular updates (at least annually). Online safety training is integrated into the school's whole-school safeguarding approach, wider staff development and curriculum planning.

- All staff will receive online safety training and understand their responsibilities under this policy.
- A planned programme of online safety, data protection and cybersecurity training for all staff, regularly updated and reinforced. Staff training needs

will be reviewed periodically to ensure provision remains relevant and effective.

- Online safety training for all new staff as part of induction, ensuring understanding of the **Online Safety Policy** and **Acceptable Use Agreements**, including classroom management, professional conduct, online reputation and modelling positive online behaviour.
- Regular updates for the Designated Safeguarding Leads through external training and review of relevant guidance (e.g. UK Safer Internet Centre, SWGfL, MAT, Local Authority or other appropriate organisations).
- Support for staff knowledge-building and consistent practice through structured professional learning resources and staff briefings.
- Regular review of this **Online Safety Policy** and updates through staff meetings, team briefings and/or INSET.
- Targeted advice, guidance and training from the DSL when required.

**Education - Governors**

Governors should take part in online safety training and awareness activity. This is particularly important for governors with responsibility for safeguarding, online safety, technology or health and safety.

- Complete online training via the school provider
- Participation in school training and information sessions (for example, staff briefings or parent events). This may include attendance at assemblies or lessons where appropriate.
- Regular update meetings with the DSL and/or Online Safety Lead to review key themes, incidents and current priorities.

Enhanced training will be provided for (at least) the Online Safety Governor. This will include:

- Basic cyber security awareness training.
- Training to understand the school's filtering and monitoring provision, enabling effective participation in required checks and reviews.

**Education - External Stakeholders**

Families, the wider community and external agencies play a vital role in supporting the online safety education and wellbeing of learners. The school recognises that parents and carers may have limited awareness of online risks, and that many external bodies can enhance the school's safeguarding approach.

The school therefore works actively to build strong partnerships, share key messages, and ensure that families and the wider community are equipped to help keep children safe online.

The following principles underpin the school's engagement with external stakeholders:

❖ **Working with Parents and Carers**

The school will support parents and carers to understand online risks, build confidence, and reinforce safe online behaviours at home. This includes:

- Regular communication and awareness-raising about online safety issues, curriculum content, and reporting routes.
- Providing information through newsletters, the school website, learning platforms, and digital communication tools.
- Offering opportunities such as parent/carer workshops, information events, or drop-ins focused on online safety.
- Involving learners in sharing online safety messages with parents/carers, including contributing to information events.
- Signposting parents and carers to trusted national resources
- Promoting and participating in key national events such as Safer Internet Day.
- Ensuring parents and carers understand acceptable use expectations and relevant school policies related to online safety.

❖ **Wider Community and Agencies**

The school recognises the value of working with external organisations to strengthen local online safety awareness and provision. This may include:

- Sharing online safety information, resources or updates with community groups, extended family members and the wider community.
- Providing or supporting family learning opportunities on digital technologies and safe online behaviours.
- Using the school website or social media channels to offer online safety content suitable for the broader community.
- Collaborating with early years settings, childminders, youth and sports groups, libraries, voluntary organisations or other local agencies.

- Drawing on the expertise of external agencies (e.g. UK Safer Internet Centre, CEOP, Local Safeguarding Partnerships, Prevent teams, police and health professionals).
- Participating in shared activities with other schools or settings, including transition projects and multi-school events.
- Supporting external groups to review and improve their own online safety practice.

## 8. Technology

The school recognises that effective filtering, monitoring, technical security, cyber security and data protection are essential to safeguarding children and protecting the wider school community. These measures support safe and responsible use of technology while enabling effective teaching, learning and administration.

The following policies have been developed and set out detailed arrangements:

- **Filtering and Monitoring Policy**
- **Technical Security Policy**

## 9. Filtering and Monitoring

The school uses Senso for filtering and monitoring, alongside the school firewall and direct staff supervision. Senso filtering and monitoring controls apply to all school computers. Mark Ozenbrook ensures their configuration, device coverage and effectiveness are checked; use of the product name alone does not demonstrate coverage.

Senso console access is restricted to Mark Ozenbrook, Shani Ozenbrook, Rebecca Jennings and Lorraine Pooley. All four have received online safety and other appropriate training. They use individual authorised accounts and access only information needed for their role. Governors and external IT contacts are not granted Senso console access by this policy.

Mark Ozenbrook manages pupil identities and account settings in Google Admin Console. James Gill at Switch Voice and Data manages the firewall. Nathan Welsh at Bloobo IT Support manages Microsoft accounts. These responsibilities are distinct from Senso console access. Providers support configuration and checks through the authorised school users and their own agreed technical roles.

Only school-approved AI may be accessed through the Senso whitelist (allow list) on all school computers. Approval records must distinguish staff demonstrations

from direct pupil use and identify the exact service, feature, URL, age/year group, purpose, permitted inputs and review date. A whitelist entry does not approve every feature or make a tool suitable for every child. New or externally linked tools within iLearn2 need their own checks before access is enabled.

Unapproved AI is blocked. Whitelist changes are approved, recorded, limited to the relevant staff or pupil profile and checked after implementation. Microsoft Copilot remains staff-operated for this school's 3-11 age range. No AI activity starts until its approval and access checks are complete.

Senso logs and filtering checks are reviewed weekly on Monday. Shani Ozenbrook and Lorraine Pooley carry out the established weekly log review, with Mark Ozenbrook accountable and Rebecca Jennings providing deputy cover. High-risk email alerts are reviewed and escalated immediately when received, rather than held for Monday. Mark ensures named cover during school use. Actions, owners, outcomes and trends are recorded in the safeguarding and technical logs as appropriate; summary assurance goes to SLT and each governing body meeting.

Staff physically supervise pupil devices and report concerns immediately. Lorraine supports log administration and alerts; the DSL or a deputy makes safeguarding decisions. Staff must not screenshot, copy or forward suspected child sexual abuse imagery; secure the device and report through safeguarding procedures.

There is a recorded effectiveness review at least once every academic year and after significant changes, incidents, new AI tools or a site move. Checks include all relevant computers, profiles, browsers, apps and connections. New or replacement devices are checked before pupil use. Any iPad, guest/BYOD or off-site limitation must be recorded and addressed before that use is permitted.

The 2026 audit records that devices are not sent home with pupils. This does not waive controls for staff devices off-site or any future remote provision. If arrangements change, they require assessment and verified protection first. Individual pupil logins remain an audit action until deployment and traceability are evidenced; interim device/session records must identify users.

Monthly keyword reviews, staff briefings, pupil voice, training and trend analysis inform improvements. Further training scheduled in the action plan remains planned until completion is recorded. Detailed responsibilities, access controls and review records are set out in the Filtering and Monitoring Policy.

**10.Technical Security**

The school takes steps to ensure that its technical infrastructure is secure, reliable and well managed and meets its statutory requirements.

The school ensures that:

- access to systems and data is controlled through appropriate authentication and permissions
- devices, networks and systems are protected through secure configuration, patching and malware protection
- backups and recovery arrangements are in place to reduce the impact of system failure or attack
- incidents and weaknesses are reported, recorded and used to inform improvement
- responsibilities for technical security are clearly defined and supported by appropriate expertise
- systems are regularly reviewed and tested, meet statutory requirements and address emerging threats.

Detailed arrangement can be found in **Technical Security Policy**.

## 11. Cyber Security

The school recognises cyber security as a leadership and governance responsibility and takes steps to reduce the risk and impact of cyber incidents.

The school ensures that:

- a cyber security approach is in place to prevent, detect, respond to and recover from cyber threats
- senior leaders and governors understand cyber risks and receive appropriate assurance
- staff and learners are educated/trained to recognise and report cyber security concerns
- business continuity and incident response arrangements are maintained and reviewed
- cyber security arrangements are kept under regular review and updated in line with emerging risks.

Detailed arrangements can be found in **Cyber Security Policy**.

## 12. Data Protection

The school is committed to protecting personal data and complying with data protection legislation.

The school ensures that:

- personal data is processed lawfully, fairly and transparently
- a Data Protection Officer (DPO) is appointed and appropriate governance arrangements are in place
- all staff receive regular training to ensure they are aware of their responsibilities and can respond appropriately to data protection incidents.
- systems are in place to respond effectively to Freedom of Information and Subject Access Requests
- privacy notices explain how data is used and how individual rights can be exercised
- data is stored, shared and disposed of securely
- data breaches are reported and managed in line with legal requirements
- data protection is embedded across safeguarding, teaching, learning and administration.

Detailed arrangements can be found in **Data Protection Policy**.

### Review

Arrangements for filtering, monitoring, technical/cyber security and data protection are reviewed regularly and updated to reflect:

- changes in technology
- emerging safeguarding risks
- national guidance and statutory expectations

## 13. Technology Practice

The school recognises that the safe and responsible day-to-day use of technology plays a vital role in safeguarding children, supporting learning, and protecting the school community. Clear expectations, consistent practice and informed users help reduce risk while enabling positive and purposeful use of digital technologies. This approach supports the safeguarding duties set out in Keeping

Children Safe in Education, emphasising safeguarding and whole-school responsibility, including the requirement to address online safety through policy, practice and education.

The following policies have been developed and set out detailed arrangements:
**Technical Security Policy**
**Public Online Communications Policy**

## 14. Device Management

The school manages the use of digital devices in a way that supports safeguarding, learning and responsible behaviour. This reflects KCSIE's requirement for a clear mobile / smart technology policy and explicitly links device use to behaviour, safeguarding and education.

The school ensures that:

- expectations for the use of school-owned and personal devices are clearly defined and communicated
- device use is consistent with safeguarding, behaviour, data protection and acceptable use policies
- appropriate technical and procedural controls are in place to support safe use
- staff are trained and visitors are informed and understand their responsibilities when using devices on school premises or systems
- education on the safe and responsible use of devices forms part of the school's online safety education

Decisions about device use are informed by risk assessment and reviewed regularly.

## 15. Digital Content

The school recognises that digital content (images, video and any other multi-modal digital media) can enrich learning and communication when used responsibly. It directly supports KCSIE expectations around sexual imagery, sharing of images, consent and coercion. It also reinforces lawful management of digital content as part of safeguarding and embeds education and prevention alongside policy.

The school ensures that:

- clear expectations are in place for the creation, use, storage and sharing of digital content
- consent, privacy and safeguarding considerations are applied consistently
- staff and learners are trained/educated to understand their responsibilities when creating or sharing digital content
- personal data and images are handled securely and lawfully
- policy and practice are reviewed in the light of emerging technologies and risks.

## 16. Public Online Communications

The school uses public online communications to inform, celebrate success and engage with the wider community, while managing associated risks. It supports KCSIE expectations around professional boundaries and staff conduct online, addresses reputational and safeguarding risk from public platforms while reinforcing parental engagement and transparency.

The school ensures that:

- public online communications are appropriate, accurate and well-managed
- public communications from or regarding the school are monitored and addressed where appropriate
- published content complies with safeguarding, data protection and statutory requirements
- to reduce the risk of illegal manipulation of publicly available images of staff and learners, the school has procedures in place to control how those images are shared online.
- online safety information is shared with parents, carers and the wider community
- clear processes exist for managing school online accounts
- staff understand expectations around professional conduct and online behaviour

## Review

Technology practice is reviewed regularly to reflect:

- changes in technology and online behaviour
- emerging safeguarding risks

- feedback from staff, learners and parents
- national guidance and statutory expectations

## 17. Outcomes

The impact of the **Online Safety Policy** and practice is evaluated regularly using evidence such as:

- ❖ online safety incident logs
- ❖ behaviour and bullying records
- ❖ surveys of staff, learners and parents/carers.

Evaluating student outcomes as part of their online safety should be defined and evaluated as part of the school's assessment processes, assessment and tracking. Findings are reported to relevant groups and used to strengthen practice. This process ensures that:

- Evidence from audits and reviews is discussed through balanced professional debate, alongside the impact of preventative work (education, awareness and training).
- Clear reporting routes are in place so patterns, themes and outcomes are shared regularly with senior leaders and governors.
- Parents/carers are informed of key patterns and learning through the school's online safety communication and awareness activity.
- Online safety and related policies and procedures are updated in response to evidence and emerging risks.
- Learning and evidence of impact are shared, where appropriate, with other schools, agencies and local authorities to support a consistent local approach to online safety

**Version control table**

| Version | Date | Changes | Approval |
|---|---|---|---|
| 1 | 2026 | Policy re-written to meet the updated requirements in KCSIE and the DfE Technical Standards for Schools and Colleges and to take account of new developments in digital technologies – particularly the use of Artificial Intelligence (AI) in schools. | GB |

| | | | |
|---|---|---|---|
| 2 | 15 November 2026 | Aligned AI, iLearn2, Senso, named roles, audit arrangements and appendix references. | Pending governing body approval |

## Appendix A – AUAs

### Acceptable Use Agreement – KS2 Learner

I agree to use the school's digital systems safely and responsibly to protect me, other learners and the school.

**Keeping Safe Online**

- The school will check how I use devices and the internet to keep everyone safe.
- I will keep my usernames and passwords private and tell a trusted adult if someone else knows them.
- I will be careful when talking to people online and will only talk to people I know and trust.
- I will not share personal information like my name, address, or photos without asking a trusted adult.
- I will only take or share images of myself, or others, when fully dressed.
- If I see or hear something online that worries or upsets me, I will tell a trusted adult straight away.
- I will only meet people I have spoken to online if a trusted adult is with me.

**Using Computers and the Internet Sensibly**

- I will only use devices, apps and sites that I am allowed to, and will check if I am unsure.
- I will always ask permission and check with a trusted adult before using someone else's work or pictures.
- I will make sure the information I find online is true by checking carefully.
- I will use AI only when my teacher has set a school-approved, age-appropriate activity and is supervising. I will not use a teacher's account or open other AI tools.
- I will not copy or use music, videos, or games unless I have permission.
- I will tell a trusted adult about any damage to devices or if anything else goes wrong.
- I will check with trusted adults before clicking on any unexpected messages or links (even if these look as though they are from people that I already know).

**Being Respectful and Responsible**

- I will treat others kindly online, just as I do in real life.
- I will make good choices about what I share online to protect myself and others.
- I will spend a healthy amount of time using devices and make time for other activities too.
- I will always think about how my behaviour online could affect me, my friends, and my school.

**What Happens If I Break These Rules?**

- If I don't follow these rules, my teacher may stop me from using computers or devices, speak to my parents, or take other actions to help me make better choices in the future.

By following these rules, I can enjoy using technology safely and responsibly.

**I have read and understand the above and agree to follow these guidelines when:**

- **I use the school systems and devices (both in and out of school)**
- **I use my own devices in the school (when allowed) e.g. mobile phones, gaming devices USB devices, cameras etc.**
- **I am out of school and involved in any online behaviour that might affect the school or other members of the school.**

| | | | |
|---|---|---|---|
| **Learner Name:** | | **Class:** | |
| **Signed:** | | **Date:** | |

**Acceptable Use Agreement – Parent/Carer**

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies provide powerful tools, which open new opportunities for everyone. They can stimulate discussion, promote creativity, and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This acceptable use policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that parents and carers are aware of the importance of online safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

The school will try to ensure that learners have good access to digital technologies to enhance their learning and will, in return, expect the learners to agree to be responsible users. A copy of the learner acceptable use agreement is attached to this permission form, so that parents/carers will be aware of the school expectations of the young people in their care.

Parents are requested to sign the permission form below to show their support of the school in this important aspect of the school's work.

**Permission Form**

| | |
|---|---|
| **Parent/Carer Name:** | |
| **Learner Name:** | |

As the parent/carer of the above learners, I give permission for my son/daughter to have access to the digital technologies at school.

I understand that the school has discussed the acceptable use agreement with my son/daughter and that they have received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

I understand that the school takes reasonable precautions, including filtering, monitoring and supervision, to protect children online. No system can prevent every exposure to unsuitable material. The school remains responsible for its safeguarding arrangements and will respond to concerns through its safeguarding procedures.

I understand that my son's/daughter's activity on the systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the acceptable use agreement.
I will encourage my child to adopt safe use of digital technologies at home and will inform the school if I have concerns over my child's online safety.

**Use of Digital/Video Images**

The use of digital/video images plays an important part in learning activities. Learners and members of staff may record evidence of activities in lessons and out of school. These images may then be used in presentations in subsequent lessons.
Images may also be used to celebrate success through their publication in newsletters, on the school website and occasionally in the public media. Where an image is publicly shared by any means, only your child's **delete as relevant** first name/initials will be used.
The school will comply with the Data Protection Act and request parent's/carer's permission before taking images of members of the school. We will also ensure that when images are published that the young people cannot be identified by the use of their names.
In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other learners in the digital/video images.
Parents/carers are requested to sign the permission form below to allow the school to take and use images of their children and for the parents/carers to agree.

**Digital/Video Images Permission Form**

| | |
|---|---|
| As the parent/carer of the above learner, I agree to the school taking digital/video images of my child/children. | Yes/No |
| I agree to these images being used: | |
| • to support learning activities. | Yes/No |
| • in publicity that reasonably celebrates success and promotes the work of the school. | Yes/No |
| Insert statements here that explicitly detail where images are published | Yes/No |

| | |
|---|---|
| by the schools | |
| I agree that if I take digital or video images at, or of school events which include images of children, other than my own, I will abide by these guidelines in my use of these images. | Yes/No |

| | |
|---|---|
| **Parent/Carer Name:** | |
| **Signed:** | |
| **Date:** | |

## Acceptable Use Agreement – Staff & Volunteer

### School Policy

Digital technologies have become integral to the lives of everyone, including children and young people, both within schools and in their lives outside school. The internet and digital technologies are powerful tools, which can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work.

The school has the right to protect itself and its systems and all users should have an entitlement to safe access to the internet and digital technologies at all times. This acceptable use policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while online and using digital technologies for educational, personal and recreational use
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk
- that staff are protected from potential risk in their use of technology in their everyday work.

The school will try to ensure that staff and volunteers will have good access to digital technology to enhance their work, to enhance learning opportunities and will, in return, expect staff and volunteers to agree to be responsible users.

### Acceptable Use Policy Agreement

I understand that I must use school systems in a responsible way, to minimise the risk to the safety, privacy or security of the school community and its systems. I acknowledge the potential of digital technologies for enhancing learning and will endeavour to integrate them in a way that aligns with the school's policy, ethos and values.

For my professional and personal safety:

- I understand that the school will monitor my use of school devices and digital technology systems
- I understand that the rules set out in this agreement also apply to use of these devices and technologies out of school, and to the transfer of personal / sensitive data (digital or paper based) out of the school
- I understand that the school devices and digital technology systems are primarily intended for educational use and that I will only use them for personal or recreational use within relevant school policies. .

- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password.
- I will store my passwords securely and in line with the school's relevant security policy.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using digital technologies and systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner. I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital/video images, and taking account of parental permissions. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the school website) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use social networking sites in the school in accordance with school policies.
- I will only communicate with learners and parents/carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any online activity that may compromise my professional responsibilities.

The school has the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- I will abide by all relevant guidance and legislation (e.g., Keeping Children Safe in Education / UK GDPR)
- I will ensure that I am aware of cyber-security risks and that I will not respond to any communications that might put my / school data or systems at risk from attack
- When using AI systems in my professional role I will use these responsibly and:

- will use only school-approved AI, accounts and activities enabled through the Senso whitelist, and follow the Generative AI Policy
- will be aware of the risks of bias and discrimination, critically evaluating the outputs of AI systems for such risks
- will not enter identifiable pupil information, images or sensitive records into AI prompts or uploads; any separately proposed pupil-data workflow requires specific approval and data protection assessment before use
- will respect copyright and intellectual property, and will not allow pupil material to be used to train AI models
- will make AI assistance clear where AI has materially supported an output and disclosure is appropriate, consistently with the Generative AI Policy
- critically evaluate AI-generated outputs to ensure that all AI-generated content is fact-checked and reviewed for accuracy before sharing or publishing
- will use generative AI tools responsibly to create authentic and beneficial content, ensuring respect for individuals' identity and well-being
- When I use my personal mobile devices in school, I will follow the rules set out by the school, in the same way as if I was using school equipment. I will ensure that any such devices are protected by up to date anti-virus / anti-malware software and are free from viruses.
- When communicating in a professional capacity, I will only use technology and systems sanctioned by the school.
- I will not use personal accounts on school systems.
- I will exercise informed safe and secure practice when accessing links to content from outside of my organisation to reduce the risk of cyber security threats.
- I will ensure that my data is regularly backed up, in accordance with relevant school policies.
- I will not access illegal, inappropriate or harmful content on school systems.
- I will not bypass any filtering or security systems that are used to prevent access to such content.
- I will not install or attempt to install unauthorised programmes of any type on a school device , nor will I try to alter device settings, unless this is allowed in school policies

- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the school Data Protection Policy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based documents containing personal data must be held in lockable storage.
- I understand that the data protection policy requires that any staff or learner data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using digital technologies in my professional capacity or for school sanctioned personal use:

- I will ensure that I have appropriate permissions to use the original work of others in my own work and will reflect this with appropriate acknowledgements, particularly where AI has been used to generate content
- Where content is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of the school:

- I understand that this acceptable use agreement applies to my use of digital technologies related to my professional responsibilities , within or outside of the school.
- I will ensure my use of technologies and platforms is in line with the school's agreed codes of conduct.
- I understand that if I fail to comply with this acceptable use agreement, I could be subject to disciplinary action. This could include (schools should amend this section to provide relevant sanctions as per their behaviour policies) a warning, a suspension, referral to Governors and/or the Local Authority / Trust in the event of illegal activities, the involvement of the Police.

**I have read and understand the above and agree to use the school digital technology systems (both in and out of the school) and my own devices (in the school and when carrying out communications related to the school) within these guidelines.**

| | |
|---|---|
| **Staff/Volunteer Name:** | |
| **Signed:** | |
| **Date:** | |

## Appendix B - Kingdom Christian School Acceptable/Unacceptable Use tables

Apply the named roles, school approval, provider age limits and safeguarding restrictions. “Selected staff” means staff authorised for that activity. In AI demonstrations, staff operate the AI and pupils may ask questions. No entry permits otherwise prohibited accounts, chat or AI features.

| User Actions | Staff and other adults | | | | Learners | | | |
|---|---|---|---|---|---|---|---|---|
| | Not allowed | Allowed | Allowed at certain times | Allowed for selected staff | Not allowed | Allowed | Allowed at certain times | Allowed with staff oversight |
| Online gaming and in-game chat/voice (*e.g. Roblox, Fortnite, Minecraft*) | | | x | | | | x | |
| Online shopping and digital commerce (*including in-app purchases, marketplaces, subscriptions)* | | | X | | x | | | |
| Cloud storage and file sharing (*e.g., Google Drive, OneDrive, Dropbox, WeTransfer; P2P/torrents*) | | X | | | | | x | |
| Social media and user-generated platforms *(e.g. TikTok, Instagram, Snapchat, X, Reddit) and other age-restricted services* | | | x | | x | | | |
| Messaging, chat and voice *(e.g., WhatsApp, iMessage, Snapchat, Discord, Teams personal accounts)* | | x | | | x | | | |
| Streaming entertainment/media (video, music, podcasts) *e.g. Netflix, Disney+, Spotify* | | x | | | | | x | |
| Video platforms and livestreaming *(e.g. YouTube, Twitch, TikTok LIVE, Instagram Live)* | | X | | | x | | | |
| Personal mobile phones and smart devices on site *(phones, smartwatches, earbuds)* | | X | | | x | | | |
| Mobile phones used for learning (teacher-directed and supervised) | | | x | | x | | | |
| Mobile phones used during social time/breaks (where permitted) including device-free approaches | | x | | | x | | | |
| Taking photos/video/audio on personal devices or sharing location data without school authorisation and required permissions | x | | | | x | | | |
| Other personal devices *(e.g., tablets, handheld consoles, VR headsets, wearables)* | x | | | | x | | | |
| Personal email accounts on site or on the school network/Wi-Fi *(e.g., Gmail, Outlook.com)* | | x | | | x | | | |
| School email used for personal communication (non-work/non-learning) | x | | | | x | | | |
| Unapproved AI tools, services, features or browser extensions | x | | | | x | | | |
| Approved AI for teacher-operated demonstrations | | | | x | x | | | |
| Approved age-appropriate iLearn2 AI activities; pupil use only with staff supervision | | | | x | | | | x |
| Senso console access: named authorised users only | | | | x | x | | | |

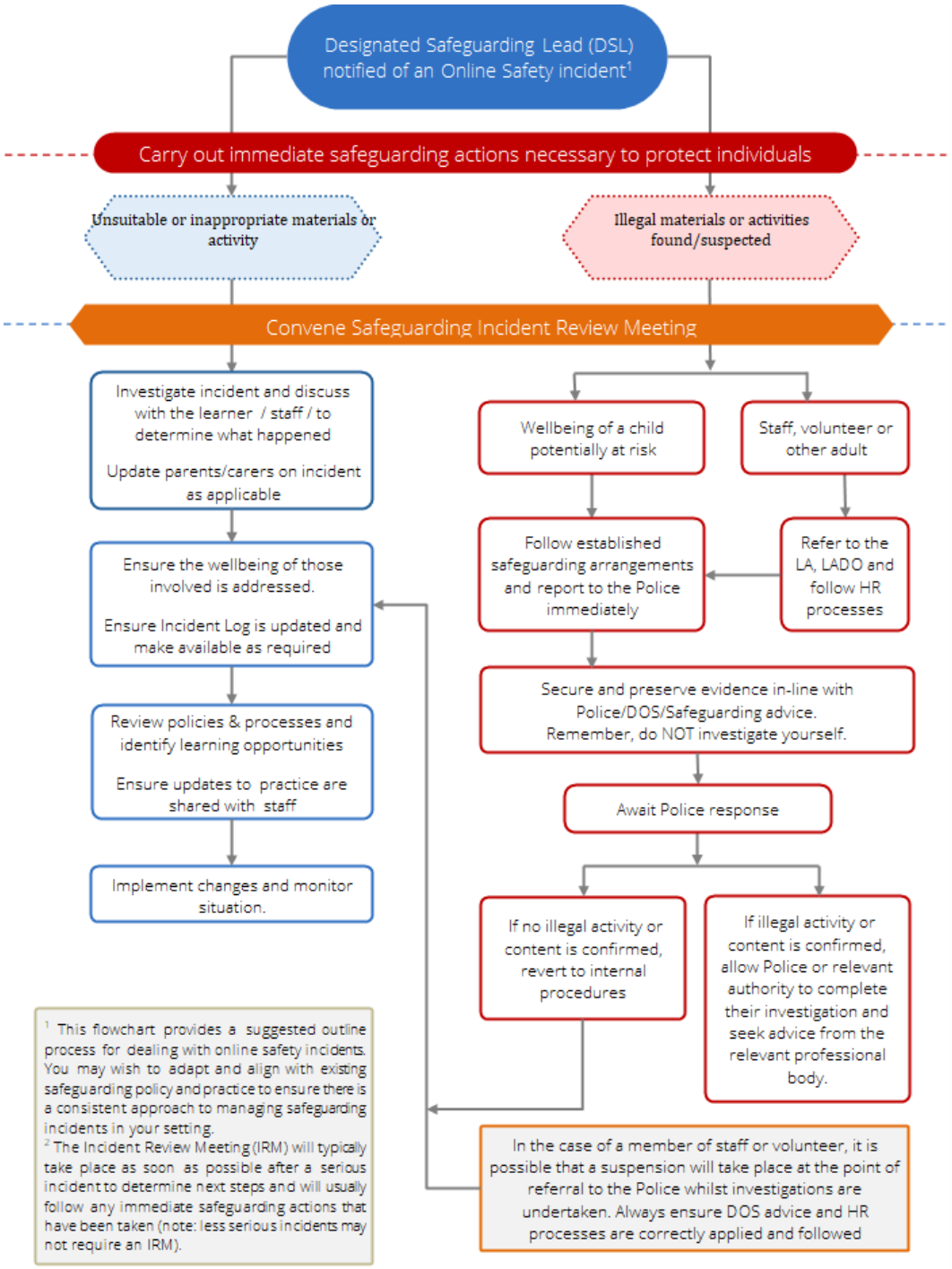
## Activities which are unacceptable or unlawful

| User actions | | Acceptable | Acceptable at certain times | Acceptable for nominated users | Unacceptable | Unacceptable and illegal |
|---|---|---|---|---|---|---|
| Users shall not access online content (including apps, games, sites) to make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to: | **Any illegal activity for example:**<br>Child sexual abuse imagery*<br>Child sexual abuse/exploitation/grooming<br>Terrorism<br>Encouraging or assisting suicide<br>Offences relating to sexual images i.e., revenge and extreme pornography<br>Incitement to and threats of violence<br>Hate crime<br>Public order offences - harassment and stalking<br>Drug-related offences<br>Weapons / firearms offences<br>Fraud and financial crime including money laundering | | | | | X |
| Users shall not undertake activities that might be classed as cyber-crime under the Computer Misuse Act (1990) | Using another individual's username or ID and password to access data, a program, or parts of a system that the user is not authorised to access (even if the initial access is authorised)<br><br>Gaining unauthorised access to school networks, data and files, through the use of computers/devices<br><br>Creating or propagating computer viruses or other harmful files<br>Revealing or publicising confidential or proprietary information (e.g., financial / personal information, databases, computer / network access codes and passwords)<br><br>Disable/Impair/Disrupt network functionality through the use of computers/devices<br>Using penetration testing equipment (without relevant permission) | | | | | X |

| User actions | | Acceptable | Acceptable at certain times | Acceptable for nominated users | Unacceptable | Unacceptable and illegal |
|---|---|---|---|---|---|---|
| Users shall not undertake activities that are not illegal but are classed as unacceptable in school policies: | Accessing inappropriate material/activities online in a school setting including pornography, gambling, drugs. (Informed by the school's filtering practices and/or AUAs) | | | | X | |
| | Promotion of any kind of discrimination | | | | X | |
| | Using school systems to run a private business | | | | X | |
| | Using systems, applications, websites or other mechanisms that bypass the filtering/monitoring or other safeguards employed by the school | | | | X | |
| | Infringing copyright and intellectual property (including through the use of AI services) | | | | X | |
| | Unfair usage (downloading/uploading large files that hinders others in their use of the internet) | | | X | X | |
| | Any other information which may be offensive to others or breaches the integrity of the ethos of the school or brings the school into disrepute | | | | X | |

## Appendix C – Flowchart: Decision-making for dealing with online safety incidents

Apply the named DSL/deputy reporting route in section 5. Urgent referrals and protective action must not wait for an incident review meeting. Follow safeguarding advice on preserving evidence; do not copy or circulate suspected illegal images.



## Appendix D – AI Risk Assessment Matrix Template

| Risk Area | Risk Description | Likelihood (L/M/H) | Impact (L/M/H) | Risk Level (L/M/H) | Mitigation Measures |
|---|---|---|---|---|---|
| Data Protection and Privacy Breaches | | | | | |
| Cyberbullying | | | | | |
| Over-reliance on AI | | | | | |
| Emotional Manipulation | | | | | |
| Inappropriate Content or Conduct | | | | | |
| Mental Health Impacts | | | | | |
| Bias and Discrimination | | | | | |
| Misuse of AI | | | | | |
| Misinformation | | | | | |
| Digital Divide | | | | | |
| AI Ethics Awareness | | | | | |
| Data Accuracy | | | | | |
| Legal Compliance | | | | | |
| Cyber-Security | | | | | |
| **Action Plan:** | | | | | |

## Appendix E – Responding to Learner Actions

Marks identify possible response routes, not automatic sanctions or referrals. The DSL assesses safeguarding needs, age, SEND, context and risk; safeguarding, allegations and behaviour/staff procedures determine the response.

| **Incidents** | Refer to class teacher | Refer to DSL/OSL | Refer to Police/Social Services | Refer to IT Services Provider | Inform parents/carers | Issue a warning/Intervention | Remove device/network/ internet/access rights | Further sanction, in line with Behaviour Policy |
|---|---|---|---|---|---|---|---|---|
| Accessing illegal material (or attempting to), as defined in the earlier "Unsuitable/Inappropriate Activities" section. | **x** | **x** | **x** | **x** | **x** | **x** | **x** | **x** |
| Damaging, corrupting or deleting another user's data | **x** | | | | | **x** | | **x** |
| Sending offensive, harassing or bullying emails, texts or messages. | **x** | **x** | | | **x** | **x** | **x** | **X** |
| Unauthorised downloading/uploading, file sharing or distribution of files. | **x** | **x** | | **x** | **x** | **x** | **x** | **X** |
| Bypassing filtering (e.g. proxy sites, VPNs or similar tools). | **x** | **x** | | **x** | **x** | **x** | **x** | **X** |
| Failing to report accidental access to offensive or pornographic material | **x** | **x** | **x** | **x** | **x** | **x** | **x** | **X** |
| Deliberately accessing offensive or pornographic material (or attempting to) | **x** | **x** | **x** | **x** | **x** | **x** | **x** | **X** |
| Sharing or receiving content that breaches copyright or data protection law. | **x** | | | | | **x** | | **X** |
| Unauthorised use of devices, including taking photos/videos or audio recordings. | **x** | **x** | | | **x** | **x** | **x** | **X** |
| Unauthorised use of online services (apps, websites or platforms). | **x** | **x** | | | **x** | **x** | **x** | **X** |
| Any online behaviour that could bring the school into disrepute or undermines the school's ethos. | **x** | **x** | | | **x** | **x** | **x** | **X** |
| Repeated breaches of these rules following previous warnings or sanctions. | **x** | **x** | | | **x** | **x** | **x** | **x** |

## Appendix F - Responding to Staff Actions

Marks identify possible response routes, not automatic sanctions or referrals. The DSL assesses safeguarding needs, age, SEND, context and risk; safeguarding, allegations and behaviour/staff procedures determine the response.

| Incidents | Refer to SLT/ Headteacher | Refer to Trustees | Refer to Police/ LADO | Refer to IT Services Provider | Issue a warning | Disciplinary action: Staff Code of Conduct |
|---|---|---|---|---|---|---|
| Accessing illegal material (or attempting to), as defined in the earlier "Unsuitable/Inappropriate Activities" section. | x | x | x | x | x | X |
| Breaching data protection or cyber-security requirements, including network security rules. | x | x | | x | x | X |
| Accessing offensive or pornographic material (or attempting to). | x | x | x | x | x | x |
| Damaging systems or data, including corrupting/deleting others' data or deliberately damaging hardware/software. | x | x | | x | x | X |
| Bypassing filtering controls (e.g. proxy sites, VPNs or similar methods). | x | x | | x | x | X |
| Unauthorised downloading, uploading or file sharing. | x | x | | x | x | X |
| Breaching copyright, licensing or intellectual property, including misuse of AI systems. | x | x | | x | x | X |
| Sending offensive, harassing or bullying emails, texts or messages. | x | x | | x | x | X |
| Use of personal email/social media/messaging to communicate with learners or parents/carers. | x | | | | X | |
| Inappropriate personal use of school technology, including personal email and social media use during work time/using school systems. | x | x | | x | x | X |

| Incidents | Refer to SLT/ Headteacher | Refer to Trustees | Refer to Police/ LADO | Refer to IT Services Provider | Issue a warning | Disciplinary action: Staff Code of Conduct |
|---|---|---|---|---|---|---|
| Mishandling personal data, including storing, displaying or transferring it insecurely.<br>Any action that undermines professional conduct or a staff member's professional standing. | x | x | | x | x | X |
| Actions which could bring the school into disrepute or breach the integrity or the ethos of the school. | x | x | | x | x | X |
| Failing to report incidents, whether accidental or deliberate. | x | x | | x | x | x |
| Repeated breaches following previous warnings or sanctions. | x | x | | x | x | x |