

CATCOTT PRIMARY



---

# CATCOTT SCHOOL

# ONLINE SAFETY POLICY

---

'...where learning takes you to greater heights...'

Approved by:

H Lintern

Date:

September 2026

Last reviewed on:

September 2026

Next review due by:

September 2027

## Table of Contents

|                                                    |                              |
|----------------------------------------------------|------------------------------|
| Introduction .....                                 | Error! Bookmark not defined. |
| Purpose of the templates.....                      | Error! Bookmark not defined. |
| Expectations and statutory context .....           | Error! Bookmark not defined. |
| Using the templates.....                           | Error! Bookmark not defined. |
| Scope of the Online Safety Policy .....            | Error! Bookmark not defined. |
| Policy development, monitoring and review.....     | Error! Bookmark not defined. |
| Schedule for approval, monitoring and review ..... | Error! Bookmark not defined. |
| Policy and leadership.....                         | Error! Bookmark not defined. |
| Responsibilities .....                             | Error! Bookmark not defined. |
| Online Safety Group .....                          | Error! Bookmark not defined. |
| Policy.....                                        | Error! Bookmark not defined. |
| Online Safety Policy.....                          | Error! Bookmark not defined. |
| Acceptable use .....                               | Error! Bookmark not defined. |
| Reporting and responding .....                     | Error! Bookmark not defined. |
| Responding to Learner Actions.....                 | Error! Bookmark not defined. |
| Responding to Staff Actions.....                   | Error! Bookmark not defined. |
| Use of Artificial Intelligence (AI) .....          | Error! Bookmark not defined. |
| Education.....                                     | Error! Bookmark not defined. |
| Online Safety Education Programme.....             | Error! Bookmark not defined. |
| Staff.....                                         | Error! Bookmark not defined. |
| Governors .....                                    | Error! Bookmark not defined. |
| External Stakeholders .....                        | Error! Bookmark not defined. |
| Working with Parents and Carers.....               | Error! Bookmark not defined. |
| Wider Community and Agencies.....                  | Error! Bookmark not defined. |
| Technology.....                                    | Error! Bookmark not defined. |
| Filtering and Monitoring.....                      | Error! Bookmark not defined. |
| Technical Security.....                            | Error! Bookmark not defined. |
| Cyber Security .....                               | Error! Bookmark not defined. |
| Data Protection.....                               | Error! Bookmark not defined. |

|                                                                                                    |                              |
|----------------------------------------------------------------------------------------------------|------------------------------|
| Technology Practice .....                                                                          | Error! Bookmark not defined. |
| Device Management .....                                                                            | Error! Bookmark not defined. |
| Digital Content.....                                                                               | Error! Bookmark not defined. |
| Public Online Communications .....                                                                 | Error! Bookmark not defined. |
| Outcomes .....                                                                                     | Error! Bookmark not defined. |
| List of appendices .....                                                                           | Error! Bookmark not defined. |
| Appendix A1- Learner Acceptable Use Agreement Template – for older learners .....                  | 30                           |
| Appendix A2 - Acceptable Use Agreement Template – for KS2 Learners .....                           | 34                           |
| Appendix A3 - Acceptable Use Agreement Template – for younger learners (EY/KS1) .....              | 37                           |
| Appendix A4 - Parent/Carer Acceptable Use Agreement Template.....                                  | 38                           |
| Appendix A5 - Staff (and Volunteer) Acceptable Use Agreement Template.....                         | 45                           |
| Appendix A6 - Acceptable Use Agreement for Community Users Template .....                          | 49                           |
| Appendix A7 - Online Safety Policy Statement .....                                                 | Error! Bookmark not defined. |
| Appendix A8 - Harmful Sexual Behaviour Policy Template .....                                       | Error! Bookmark not defined. |
| Appendix A9 – Computer Misuse and Cyber Choices Policy Template                                    | Error! Bookmark not defined. |
| Appendix A10 Responding to incidents of misuse – flow chart                                        | Error! Bookmark not defined. |
| Appendix A11 - Record of reviewing devices/internet sites (responding to incidents of misuse)..... | Error! Bookmark not defined. |
| Appendix A12 - Reporting Log.....                                                                  | Error! Bookmark not defined. |
| Appendix B1 - Training Needs Audit Log .....                                                       | Error! Bookmark not defined. |
| Appendix C1 – Filtering and Monitoring Policy Template .....                                       | Error! Bookmark not defined. |
| Appendix C2 - Technical Security Template Policy .....                                             | Error! Bookmark not defined. |
| Appendix C3 - Cyber Security Policy Template.....                                                  | Error! Bookmark not defined. |
| Appendix C4 - Data Security Policy Template .....                                                  | Error! Bookmark not defined. |
| Appendix C5 – Electronic Devices: Searching, Screening and Confiscation Policy Template .....      | Error! Bookmark not defined. |
| Appendix C6 – Public Online Communications Policy Template                                         | Error! Bookmark not defined. |
| Appendix C7 - School Online Safety Policy Template – Artificial Intelligence in Schools ..         | Error! Bookmark not defined. |
| Legislation .....                                                                                  | Error! Bookmark not defined. |

Links to other organisations or documents..... Error! Bookmark not defined.

## Introduction

These Online Safety Policy templates were significantly updated in March 2026. They were completely rewritten and are now more focussed, with more accessible language and reduced in length. Schools are recommended to customise this new policy to their own needs, rather than trying to edit the previous version. In addition further edits have been made in July 2026 to reflect the updates in the 2026 Keeping Children Safe in Education guidance – these are highlighted in green

## Purpose of the templates

These policy templates are designed to support school leaders and governing bodies to produce an Online Safety Policy that is fit for purpose, proportionate, and grounded in a whole-school approach. The templates are intended to sit alongside, and align with, key policies including Safeguarding/Child Protection, Behaviour, and Anti-Bullying.

Online safety is part of a school's wider duty of care. Through an effective Online Safety Policy, schools meet statutory obligations to safeguard learners from harm within and outside school and strengthen the school's position in relation to accountability and legal challenge arising from the use of digital technology.

## Expectations and statutory context

An effective Online Safety Policy must be tailored to the needs of each school. Consultation and discussion with staff, learners, governors and, where appropriate, parents/carers, is a vital part of writing or reviewing the policy.

Schools must review their Online Safety Policy at least annually, (KCSIE Para 121) and more frequently where there are significant changes in technology, risks, or technology-related behaviours. The policy should be available publicly either via the school website or by other means.

[Keeping Children Safe in Education](#) (KCSIE) requires Local Authorities, Multi-Academy Trusts and schools to ensure children are safeguarded from harmful and inappropriate online material, and that online safety is a running and interrelated theme across the whole-school safeguarding approach. This includes how online safety is reflected in relevant policies, the curriculum, staff training, the role of the DSL (and deputies), and parental

engagement. KCSIE also recommends an annual review supported by a risk assessment; schools should use the [360 safe self-review tool](#) to support this process.

KCSIE (Para 163 – updated July 2026) describes online safety risks across four broad areas:

- Content: - being exposed to illegal, inappropriate, or harmful content, for example: pornography, racism, misogyny, self-harm, suicide, antisemitism, radicalisation, extremism, extreme sexual or physical violence, misinformation, disinformation (including fake news) and conspiracy theories,
- Contact: being subjected to harmful online interaction with other users or generative AI applications that simulate this; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- Conduct: behaviour that increases likelihood of harm for example, making, sending and receiving explicit images, including those generated using AI and online bullying, and
- Commerce: risks such as gambling, inappropriate advertising, phishing and financial scams

Schools in England are subject to increased scrutiny of online safety through inspection, and the Counter Terrorism and Security Act 2015 requires schools to protect learners from terrorist and extremist material online.

## Using the templates

With optional statements and guidance notes, this portfolio is longer than the policy a school will typically publish. It is designed to help schools address a complex and fast-changing area while producing a final policy that is concise, accessible, and widely understood.

The first part of the document provides the main Online Safety Policy Template. Appendices include further and more detailed policy templates e.g., Acceptable Use Agreements. Schools can select, adapt and adopt the sections that best meet their needs.

For clarity throughout, the term school includes academies; learner refers to children and Headteacher includes Headteachers and Principals.

## Scope of the Online Safety Policy

This Online Safety Policy sets out how *Catcott Primary 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).

Where online safety concerns or incidents occur outside school and are known to the school, *Catcott Primary 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.

### Monitoring the impact of the policy

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

- Logs of reported online safety incidents
- Filtering and monitoring records
- Reviews of the effectiveness of the filtering systems
- Internal network activity monitoring data
- Surveys/questionnaires (as appropriate) of: Learners, Parents/carers, Staff

## Policy and 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 and 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.

Lead teachers will:

- Ensure the school meets its safeguarding duty of care, including online safety.
- Know and apply procedures for serious allegations involving staff (Headteacher plus at least one senior leader).
- Ensure that the DSL, IT provider/technical staff and relevant colleagues are trained and able to fulfil their roles.
- Ensure that all staff receive appropriate online safety training which, amongst other things, includes an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring
- ensure that children are taught about how to keep themselves and others safe online, recognising that effective education will be tailored to the specific needs and vulnerabilities of individual children.
- 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.

## **Governors**

Governors approve the Online Safety Policy and challenge its effectiveness. KCSIE requires them to:

- Ensure that all staff undergo safeguarding and child protection training (including online safety which, amongst other things, includes an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring – at induction and regularly updated
- Ensure that children be taught about safeguarding, including in relation to online safety
- Review the DfE Filtering and Monitoring Standards and discuss with IT staff and service providers what more needs to be done to support the school in meeting this standard

The governing body will nominate an Online Safety Governor who will:

- Meet regularly with the DSL
- Receive anonymised incident and monitoring summaries.
- Check delivery of key commitments (e.g., education, reporting, staff training).

- Have an understanding of filtering and monitoring and through regular review, assess the effectiveness of filtering and monitoring with SLT, DSL and IT provider, in line with KCSIE and DfE Filtering and Monitoring standards.
- Report to the relevant governor group/committee:
- 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 (Para 125) states that the DSL leads safeguarding and child protection, including online safety, and understands filtering and monitoring systems and processes. KCSIE requires this to be explicit in the DSL's job description.

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 anonymised incident patterns and filtering/monitoring information.
- With the IT provider lead (at least annual) review of the effectiveness of filtering and monitoring systems and ensure that these are recorded
- Report regularly to SLT and drive continuous improvement across relevant policies and practice, using evidence (e.g. incident data, monitoring, self-review such as 360 safe).
- Ensure appropriate support for learners with SEND.

*An Online Safety Lead (OSL) may support delivery; the DSL retains lead responsibility.*

### **Online Safety Lead (OSL)**

The OSL will:

- Lead the Online Safety Group and support the DSL day to day.
- Lead development and review of online safety documentation.
- Coordinate awareness, staff confidence and reporting readiness through appropriate training

- Work with curriculum leads to map, embed and evaluate online safety education.
- Liaise with IT and pastoral/support teams.
- Maintain current knowledge of risks across content, contact, conduct and commerce.

### **Curriculum Leads**

Curriculum leads will work with the DSL to deliver a planned online safety programme (e.g. [ProjectEVOLVE](#)) 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/Child Protection Policy, Technical Security Policy and sign/comply with the Staff AUA.
- 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 / technical staff**

The IT provider supports leaders and the DSL to meet DfE filtering, monitoring and technical standards. Where services are outsourced, the school remains accountable.

The IT provider will:

- Maintain secure infrastructure and managed user access.
- Implement, maintain and update filtering and monitoring; provide reports; act on alerts and concerns.
- Support procurement, risk identification, reviews and checks with SLT/DSL.
- Monitor systems for misuse and report concerns promptly to the [Headteacher](#)

- Follow the school's Online Safety and Technical Security policies and keep technical knowledge current.

## **Learners**

Learners will:

- Follow the Learner AUA and 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.
- Use AI responsibly: protect original work, check accuracy and avoid plagiarism.
- 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 and share the learner AUA
- 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).

## **Community users**

Community users accessing school systems or platforms will sign a Community User AUA before access is provided. The school welcomes partnership working and shares good practice where appropriate.

# **Policy**

## **Online Safety Policy**

The Online Safety Policy is part of the school safeguarding framework and should be read alongside Safeguarding/Child Protection, Behaviour, Anti-Bullying and Data Protection policies.

### **What the policy does**

- 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.

### **Implementation, monitoring and review**

- Developed through the Online Safety Group and reviewed at least annually (KCSIE Para 121) , and sooner if risks/technology change.
- Monitored by the DSL/OSL and governors using anonymised incident trends, filtering/monitoring reports and education review activity (e.g. [360 safe](#), [ProjectEVOLVE](#)).
- Findings inform improvement planning and staff training priorities.

### **Communication and accessibility**

- Shared at staff induction and reinforced through training.
- Communicated to learners and parents/carers through AUAs and awareness activity.
- Published on the school website.

## **Acceptable use**

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

### **Reinforcement**

- 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

## Acceptable/Unacceptable Actions

Schools should agree what is acceptable/unacceptable for their context (age, setting and systems) and record this in the tables below.

| User actions                                                                                                                                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Acceptable | Acceptable at certain times | Acceptable for nominated users | Unacceptable | Unacceptable & illegal |
|----------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|-----------------------------|--------------------------------|--------------|------------------------|
| Users must not use online services (apps, games, sites) to create, share, download, upload, transfer or communicate material or comments that are: | <p>Any illegal activity, for example:</p> <ul style="list-style-type: none"> <li>• Child sexual abuse imagery (CSAM)*</li> <li>• Child sexual abuse/exploitation and grooming</li> <li>• Terrorism-related content</li> <li>• Encouraging, promoting or assisting suicide/self-harm</li> <li>• Sexual image offences (including intimate image abuse/revenge porn and extreme pornography)</li> <li>• Incitement to, or threats of, violence</li> <li>• Hate crime</li> <li>• Public order offences (including harassment and stalking)</li> <li>• Drug-related offences</li> <li>• Weapons/firearms offences</li> <li>• Fraud and financial crime (including money laundering)</li> <li>• <i>Note: follow UKSIC and UKCIS guidance when responding to self-generated intimate images (SGII).</i></li> </ul> |            |                             |                                |              | X                      |
| Users must not attempt or support cybercrime (Computer Misuse Act 1990), including:                                                                | <ul style="list-style-type: none"> <li>• Misusing someone else's username/ID or password to access data, software or systems without authorisation</li> <li>• Gaining unauthorised access to school networks, data or files (including bypassing security controls)</li> <li>• Creating, introducing or spreading malware (viruses, ransomware, harmful scripts)</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                  |            |                             |                                |              | X                      |

| User actions                                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | Acceptable | Acceptable at certain times | Acceptable for nominated users | Unacceptable | Unacceptable & illegal |
|----------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|-----------------------------|--------------------------------|--------------|------------------------|
|                                                                | <ul style="list-style-type: none"> <li>Phishing, credential theft, or attempting to capture passwords or personal data</li> <li>Revealing, copying or publishing confidential information (e.g., personal/financial data, databases, access codes)</li> <li>Disabling, impairing or disrupting network/services (e.g., denial of service)</li> <li>Using penetration-testing tools without explicit permission</li> </ul> <p><i>Note: schools should decide whether incidents are dealt with internally or reported to police. Serious or repeat offences should be reported. The National Crime Agency provides routes to divert young people away from cybercrime and into positive pathways.</i></p> |            |                             |                                |              |                        |
| Unacceptable (not illegal) under school policies, for example: | Accessing inappropriate material/activities online in a school setting including pornography, gambling, drugs. (Informed by the school's filtering practices and/or AUAs)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |            |                             | X                              | X            |                        |
|                                                                | Promoting discrimination, harassment or hateful content                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |            |                             |                                | X            |                        |
|                                                                | Using school systems to run a private business or make unauthorised financial gain                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |            |                             |                                | X            |                        |
|                                                                | Using tools/services to bypass filtering, monitoring or other safeguards (e.g., VPN/proxy, anonymisers, alternative DNS)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |            |                             |                                | X            |                        |
|                                                                | Infringing copyright or intellectual property (including via AI tools, stream ripping or unauthorised copying/sharing)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |            |                             |                                | X            |                        |
|                                                                | Unfair usage (downloading/uploading large files that hinders others in their use of the internet)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |            |                             | X                              | X            |                        |

| User actions |                                                                                                                           | Acceptable | Acceptable at certain times | Acceptable for nominated users | Unacceptable | Unacceptable & illegal |
|--------------|---------------------------------------------------------------------------------------------------------------------------|------------|-----------------------------|--------------------------------|--------------|------------------------|
|              | Sharing content that is offensive, undermines the school's ethos, breaches integrity, or brings the school into disrepute |            |                             |                                | X            |                        |

## Reporting and responding

### Introduction

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)*, 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. KCSIE suggests that staff should have a professional curiosity and speak to the designated safeguarding lead (or a deputy) if they have concerns about a child

## Reporting Concerns

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 child protection, whistleblowing, managing allegations and complaints policies.
- Multiple reporting options are available, such as speaking with the Designated Safeguarding Lead (DSL), online or anonymous reporting tools (e.g., Whisper), 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:

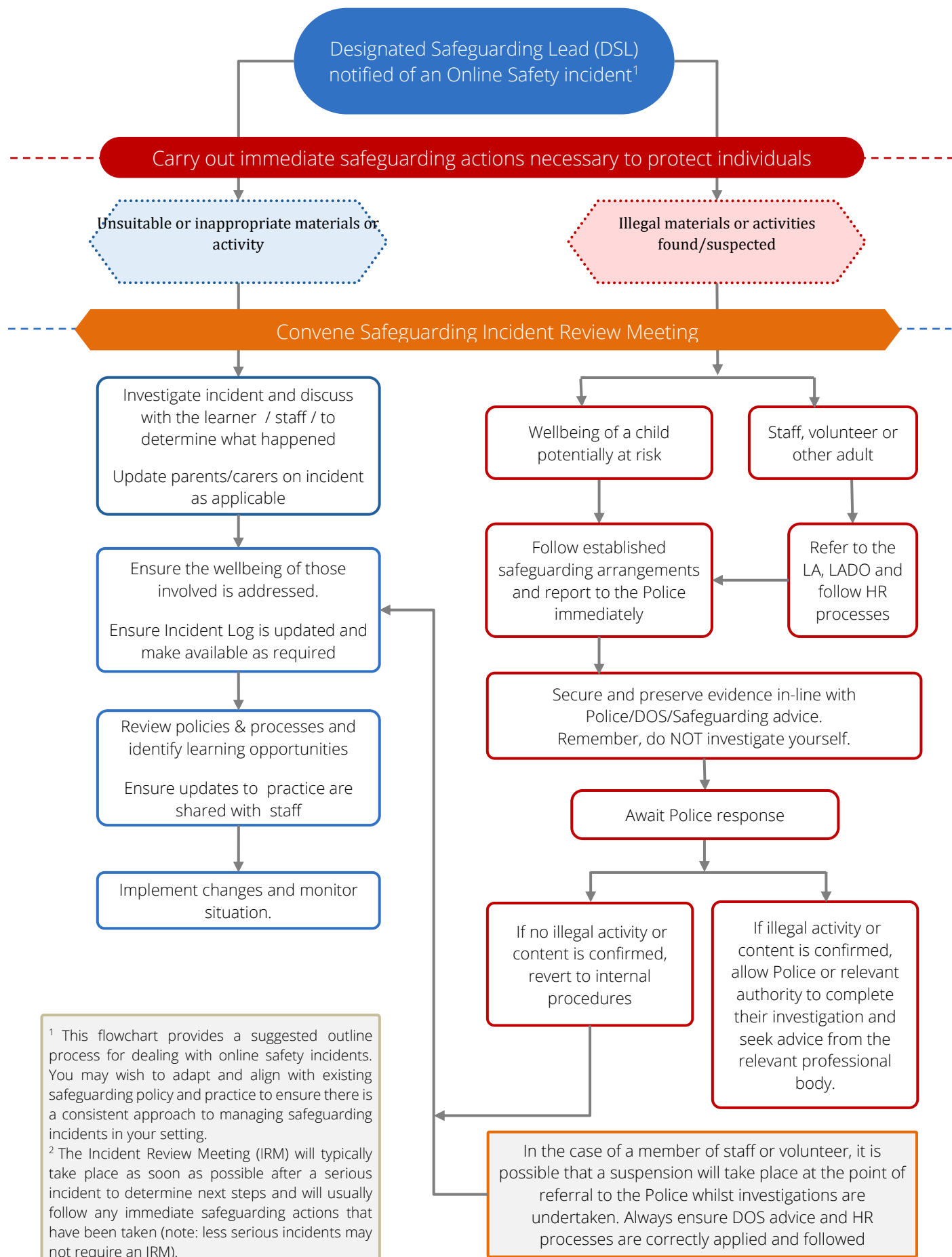
- Maintain a secure and confidential record of all incidents, including actions, decisions, and follow-up.
- Ensure reports are audited and analysed regularly to identify emerging trends, patterns of concern, and the effectiveness of responses.
- Provide anonymised summaries of trends and learning to: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

The school will make the flowchart below available to staff to support the decision-making process for dealing with online safety incidents. It was updated in January 2025. There is little change to the content, but the flowchart has been re-designed to make it easier for schools to edit. Schools are recommended to replace previous versions with this.



## Use of Artificial Intelligence (AI)

Generative AI (Gen AI) is developing rapidly and its use in education is increasing. In schools, AI is typically used in three areas: learner support, teacher support, and school operations. All use must be safe, ethical and responsible.

We recognise that Gen AI can introduce risks. These risks can be reduced through our existing safeguarding, data protection and technical security arrangements, and by updating procedures where needed. Safeguarding of learners and staff remains central to our approach.

KCSIE 2026 recognises that learners may be subject to harmful online interaction with other users or generative AI applications that simulate these.

---

### Policy statements

The school will:

- Support appropriate use of AI to enhance learning and teaching, improve outcomes, streamline administration and reduce workload. Staff remain professionally responsible and accountable for any work supported by AI.
- Comply with relevant law and guidance, including Keeping Children Safe in Education (KCSIE) and UK GDPR.
- Provide training and guidance for staff and governors on the benefits, risks and safe use of AI, and identify further development needs.
- Teach about AI through the curriculum where appropriate, helping learners understand how Gen AI works, its benefits and limitations, and its ethical and social impacts.

### Safe use, data protection and security

The school will:

- Protect personal and sensitive data. Staff must not enter personally identifiable or sensitive information into AI tools. Where AI is used, staff should use anonymised data only.
- Require UK GDPR compliance. Staff must ensure any AI tool used meets data protection and security requirements before use.

- Approve tools and accounts. Only school-approved AI tools may be used for schoolwork, and staff should use school-provided AI accounts where available to support oversight and reduce risk.
- Safeguard sensitive information. Internal documents, strategic plans or other sensitive material must not be entered into third-party AI tools unless the tool and purpose have been explicitly approved.

### **Quality, fairness and integrity**

The school will:

- Maintain human oversight. AI may support work but must not replace professional judgement—especially in decisions that affect people. AI outputs must be checked for accuracy before sharing or publishing.
- Promote transparency. Where AI has materially supported an output (e.g. documents, presentations, communications), staff should make this clear where appropriate.
- Address bias and discrimination. We recognise AI outputs may reflect bias. The school will use appropriate safeguards, review processes and procurement checks to prioritise fairness and safety.
- Protect copyright and intellectual property. The school will take steps to avoid copyright infringement and protect the intellectual property of staff and learners, including ensuring learners' work is not used to train AI systems without appropriate consent.

### **Reporting, monitoring and accountability**

The school will:

- Require prompt reporting of AI-related concerns, including misuse, data incidents or inappropriate outputs.
- Maintain an inventory of AI tools in use, with purposes and risks recorded, and carry out regular review using the risk assessment matrices in Appendix C7.
- Engage parents/carers with clear information about how AI is used in school

### **Use in assessment and feedback**

AI tools may be used to support teachers with assessment processes (e.g. identifying areas for improvement and drafting feedback), and to support learners in improving their work. Teachers remain responsible for outcomes and must ensure accuracy, fairness and appropriate use.

### **Misuse and disciplinary action**

Improper use of AI—including breaches of this policy, data protection failures, misuse of sensitive information, or failure to follow agreed processes—may result in action under the school's Staff Disciplinary Policy.

## **Education**

### **Online Safety Education Programme**

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"](#), and resources such as [SWGfL ProjectEVOLVE](#)). Learning is age-appropriate, builds on prior learning, is matched to need, and is taught through existing curriculum areas (including RSHE/RSE, Health Education, Computing and Citizenship), 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, sexual harassment and sexual violence (including online), 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](#)).

Where internet use is planned, learners are guided to appropriate resources and supported if unsuitable content is encountered. Where open searching is permitted, staff

supervise and remain vigilant. Filtering may be temporarily adjusted for legitimate curriculum research, with auditable approval and clear rationale.

Learner voice is actively used to strengthen the school's approach through feedback, learner representation (e.g. on an Online Safety Group), and opportunities such as digital leaders, peer mentoring, campaigns, and contribution to acceptable use and community-facing online safety activities.

## Staff

In line with [DfE Keeping Children Safe in Education \(KCSIE\)](#), 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. Training will include (select/delete as appropriate):
- 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.
- An understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring (KCSIE 2026)
- 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 Lead and Online Safety Lead (or other nominated staff) 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 (e.g. [ProjectEVOLVE EDU](#)) and, where appropriate, enhanced pathways (e.g. [ProjectEVOLVE SAFEGUARDING](#)).
- 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/OSL (or nominated staff) to individuals as required.

## Governors

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

Training and updates may be provided through (select/delete as appropriate):

- Attendance at training offered by the Local Authority
- 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.

## 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 (e.g. [UK Safer Internet Centre](#), [Internet Matters](#), [Childnet](#), [SWGfL](#)).
- 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, including through recommended tools such as 360 Early Years or 360 Groups.

## Technology

### Purpose

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.

Detailed arrangements are set out in the Appendix C1 - Filtering and Monitoring Policy Template and Appendix C2 - Technical Security Policy Template.

## Filtering and Monitoring

The school has appropriate filtering and monitoring systems in place to help protect users from illegal, inappropriate and harmful online content and activity, in line with statutory guidance. (e.g., [DfE Technical Standards](#), DfE [Generative AI: product safety standards](#); [KCSIE](#)) and best practice guidance (e.g., [UKSIC Appropriate Filtering and Monitoring](#)). The leadership team and relevant staff have an awareness and understanding of the provisions in place and manage them effectively and know how to escalate concerns when identified.

### The school ensures that:

- filtering and monitoring arrangements are safeguarding-led, proportionate and regularly reviewed
- filtering blocks illegal content and provides age-appropriate and role-appropriate access
- monitoring supports the rapid identification of safeguarding concerns and enables timely intervention
- all school-owned devices are subject to filtering and monitoring, including when used off-site
- staff and learners understand that filtering and monitoring are in place, why they are needed, and how concerns are escalated
- where the use of personal devices is allowed, users understand that their use may be filtered and monitored by the school.
- where Generative AI products are used they must effectively and reliably prevent users from accessing harmful or inappropriate content and filtering mechanisms should be embedded within these products
- the technical limitations of the filtering system are understood, including whether the solution can monitor and filter real-time, dynamic, personalised or AI-generated content

### Oversight and Review

- Senior leaders, the Designated Safeguarding Lead (DSL), technical staff and governors have clear roles and responsibilities

- Governors will review the DfE Filtering and Monitoring Standards and discuss with IT staff and service providers what needs to be done to support the school in meeting this standard.
- filtering and monitoring effectiveness is reviewed at least annually, and following significant changes or incidents. (e.g., using [Testfiltering](#)). Reviews will be carried out by the SLT member responsible for filtering and monitoring, with the support of the school's designated safeguarding lead and IT support. The review will include checks that filtering is working appropriately on all internet-connected devices in all relevant locations. Record of these checks will be kept and will include: when checks were conducted; which devices and environments were tested, issues identified and actions taken.
- log reports provide actionable information for safeguarding decisions.
- no system is relied upon in isolation; reporting routes and professional judgement remain central

Further detail is provided in the Appendix C1 - Filtering and Monitoring Policy Template

## 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.

Further detail is provided in the Appendix C2 - Technical Security Policy Template.

## 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. (KCSIE 2026 refers to the [DfE Cyber Security Standards](#) and recognises cyber security as a safeguarding issue).

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 their safeguarding implications 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.

## Data Protection

The school is committed to protecting personal data and complying with data protection legislation. ([The Data \(Use and Access\) Act 2025](#) makes additional requirements on schools – particularly that online services accessed by pupils meet higher protection standards)

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
- Data Protection Impact Assessments have been conducted on existing and planned use of software and systems.
- 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

- where AI and Automated Decision-Making are in use, human oversight will be maintained for significant decisions, risk assessments will be conducted and the school will ensure automated systems are transparent and explainable.

Further detail is provided in the Appendix C4 – Data Protection Policy Template.

### **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

## **Technology Practice**

### **Purpose**

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.

Detailed arrangements are set out in the Appendix C2 - Technical Security Policy Template and Appendix C6 – Public Online Communications Policy Template

## **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, learners and visitors have been trained/educated/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
- In line with the [DfE statutory guidance](#), the school prohibits for learners the use of mobile phones and other smart technology with similar functionality to mobile throughout the school day, including during lessons, the time between lessons, breaktimes and lunchtime.

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

## 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.

## 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. It has considered the risks of AI manipulation of images as highlighted in the UK Online Harms Early Warning group guidance on [Protecting your setting's images from AI](#)

## manipulation and abuse

### **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. ([guidance is available from UKSIC](#))
- 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

## **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, and 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 (e.g. using [ProjectEVOLVE Knowledge Maps](#) 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

## List of appendices

Copies of the more detailed template policies and agreements, contained in the appendix, can be found in the links and resources section of the relevant aspects in the 360safe self-review tool and online on the [SWGfL website](#). The appendices are as follows:

- A1 - Learner Acceptable Use Agreement Template – for older learners
- A2 - Learner Acceptable Use Agreement Template – KS2
- A3 - Learner Acceptable Use Agreement Template – for younger learners (EY/KS1)
- A4 - Parent/Carer Acceptable Use Agreement Template
- A5 - Staff (and Volunteer) Acceptable Use Policy Agreement Template
- A6 - Community Users Acceptable Use Agreement Template

## Appendix A1- Learner Acceptable Use Agreement Template – for older learners

Sections that include advice or guidance are written in BLUE. Schools should review and amend the contents of this agreement to ensure that it is consistent with their online safety policy and other relevant school policies.

**This acceptable use agreement is intended to ensure:**

- that young people will be responsible users and stay safe while using the internet and other 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 will have good access to digital

technologies to enhance their learning and will, in return, expect the learners to agree to be responsible users.

### **Learner Acceptable Use Agreement Form**

I agree to use the school's digital systems responsibly to protect my safety, the security of the school systems, and others.

#### **Personal Safety**

- The school will monitor my use of its digital systems, devices, and communications.
- I will keep my usernames and passwords secure and private. If compromised, I will report or change them immediately.
- I will only share personal information, like my name or address, when absolutely necessary and with permission.
- I will be cautious when meeting online contacts in person, only doing so with a trusted adult in a public place.
- I will take responsibility for my actions online, using tools like blocking or ending chats if needed.
- I will share images of myself or others only when it is safe and will ensure the images are appropriate and respectful.
- I will only take or share images of myself, or others, when fully dressed. I understand that sharing nude or semi-nude content can cause distress, may be illegal and could lead to prosecution / criminal records.
- I will report harmful or unpleasant material, messages, or anything that worries or upsets me to a trusted adult.
- 

#### **Respecting Others' Work and Information**

- I will seek permission before using or adapting someone else's work.
- I will verify information I find online, as it may not always be accurate or truthful.
- I will only use Artificial Intelligence (AI) tools approved by the school and ensure my use is ethical, legal, and transparent.
- I will fact-check and critically evaluate AI-generated content for accuracy, bias, and discrimination before sharing or publishing.
- I will avoid downloading or using copyrighted or protected materials without proper permissions.

#### **Responsible Online Behaviour**

- I will be polite and responsible when I communicate with others. I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not bully, harass, threaten, upset or make fun of others.
- I will only use platforms or software approved by the school and will not attempt to bypass the filtering/security systems in place. If I become aware of any such attempts, I will report this to a trusted adult.
- I understand cybersecurity poses a risk to both me, other learners and the school and will ensure I take precautions before accessing emails, messages or links. I will check with trusted adults if I have any such concerns.
- I will immediately report any damage, faults or failings involving equipment or software, however this may have happened.
- I will follow the age requirements for social media, apps, and tools.
- I will balance my online and offline activities to promote a healthy lifestyle.
- I will protect my online reputation and that of the school, its staff, and other learners.
- I will ensure my behaviour reflects positively on the school, both in and out of school settings.
- I understand that some online behaviours might be regarded, by some, as fun but can have serious consequences – this might include taking (or sharing) images/videos of staff, fights, learners in embarrassing situations or the setting up of fake accounts.

### Consequences of Misuse

- I understand that failing to follow this agreement may lead to consequences, including loss of access to the school's systems, detentions, suspensions, contacting parents/carers, or involvement of the police in serious cases.

By following these guidelines, I will contribute to a safe, respectful, and productive online environment.

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

- I use the school's systems and devices (both in and out of school)
- I use my own devices in the school (when allowed)
- I use digital technologies out of the school in a way that is related to me being a member of this school e.g. communicating with other members of the school, accessing school email, website etc.

(Schools will need to decide if they require learners to sign, or whether they wish to simply make them aware of acceptable use through education programmes/awareness raising).

Name of Learner: ..... Group/Class:.....  
.....

Signed: ..... Date: .....  
.....

**Parent/Carer Countersignature (optional)**

It is for schools to decide whether or not they require parents/carers to sign the parent/carers acceptable use agreement (see template later in this document). This includes a number of other permission forms (including digital and video images/biometric permission/cloud computing permission).

Some schools may, instead, wish to add a countersignature box for parents/carers to this learner acceptable use agreement.

## Appendix A2 - Acceptable Use Agreement Template – for KS2 Learners

Sections that include advice or guidance are written in BLUE. Schools should review and amend the contents of this agreement to ensure that it is consistent with their online safety policy and other relevant school policies.

This acceptable use agreement is intended:

- to ensure that learners will have good access to devices and online content, be responsible users and stay safe while using digital technologies for educational, personal and recreational use
- to help learners understand good online behaviours that they can use in school, but also outside school
- to protect school devices and networks from accidental or deliberate misuse that could put the security of the systems and users at risk.

### Acceptable Use Agreement

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 only use apps or tools, like AI, that my teacher has said are OK, and I will ask for help if I'm unsure.
- 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.

Name of Learner: ..... Group/Class:.....  
 .....

Signed: ..... Date: .....  
 .....

Schools will need to decide if they require learners to sign, or whether they wish to simply make them aware through education programmes/awareness raising.

**Parent/Carer Countersignature** (optional)

It is for schools to decide whether or not they require parents/carers to sign the parent/carers acceptable use agreement (see template later in this document in the Parent/Carer AUA). This includes a number of other permission forms (including digital and video images/biometric permission/cloud computing permission).

Some schools may, instead, wish to add a countersignature box for parents/carers to this learner acceptable use agreement.

## Appendix A3 - Acceptable Use Agreement Template – for younger learners (EY/KS1)

### Our Technology Rules

I will follow these rules to use computers, tablets and the internet safely at school. These rules help us all stay safe and have fun using computers and tablets at school!

### Staying Safe

- My teacher will watch what I do on computers, tablets and the internet to keep me safe.
- I will keep my passwords secret and tell my teacher if I need help.
- I understand that people online are not always who they say they are. I will only talk to people online if my teacher or a trusted adult says it's OK.
- I will not share my name, address, or pictures without asking my teacher or a trusted adult first.
- If I see something that makes me feel worried or upset, I will tell my teacher or a trusted adult straight away.
- I will only use apps, games or websites my teacher says are safe.

### Using Technology Kindly

- I will be kind when using technology, just like I am in real life.
- I will take care of the computers and tablets I use.
- I will only look at things my teacher says are OK.

### Making Good Choices

- I will ask my teacher before I use someone else's pictures or work.
- I will take breaks from screens and do other fun things too.
- I know that I can say no / please stop to anyone online who makes me feel sad, uncomfortable, embarrassed or upset.
- I will ask for help from a trusted adult if I am not sure what to do or if I think I may have done something wrong.

### What Happens If I Forget the Rules

- If I forget the rules, my teacher will help me learn to make better choices next time.

Signed (child): .....

(The school will need to decide whether or not they wish the children to sign the agreement – and at which age - for younger children the signature of a parent/carer should be sufficient)

Signed (parent): .....

## Appendix A4 - Parent/Carer Acceptable Use Agreement Template

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. (Schools will need to decide whether they wish parents to sign the acceptable use agreement on behalf of their child)

### Permission Form

Parent/Carers 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 will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using devices.

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.

As the schools is collecting personal data by issuing this form, it should inform parents/carers as to:

|                                        |
|----------------------------------------|
| This form (electronic or printed)      |
| Who will have access to this form.     |
| Where this form will be stored.        |
| How long this form will be stored for. |
| How this form will be destroyed.       |

Signed: .....

Date: .....

## 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 is 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.

As the school is collecting personal data by issuing this form, it should inform parents/carers as to:

|                                        |                                                                                                                             |
|----------------------------------------|-----------------------------------------------------------------------------------------------------------------------------|
| This form (electronic or printed)      | The images                                                                                                                  |
| Who will have access to this form.     | Where the images may be published. Such e.g., Social Media, website, local press, etc. (see relevant section of form below) |
| Where this form will be stored.        | Who will have access to the images.                                                                                         |
| How long this form will be stored for. | Where the images will be stored and for how long                                                                            |
| How this form will be destroyed.       | How the images will be destroyed.                                                                                           |

|  |                                                       |
|--|-------------------------------------------------------|
|  | How a request for deletion of the images can be made. |
|--|-------------------------------------------------------|

## Digital/Video Images Permission Form

Parent/Carers Name:.....Learner Name:.....

|                                                                                                                                                                                         |        |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------|
| 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:                                                                                                                                                     |        |
| <ul style="list-style-type: none"> <li>to support learning activities.</li> </ul>                                                                                                       | Yes/No |
| <ul style="list-style-type: none"> <li>in publicity that reasonably celebrates success and promotes the work of the school.</li> </ul>                                                  | Yes/No |
| Insert statements here that explicitly detail where images are published by the schools                                                                                                 | Yes/No |
| 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 |

Signed: .....

Date: .....

## Use of Cloud Systems Permission Form

Schools that use cloud hosting services may be required to seek parental permission to set up an account for learners.

Schools will need to review and amend the section below, depending on which cloud hosted services are used.

The school uses *\*insert cloud service provider name\** for learners and staff. This permission form describes the tools and learner responsibilities for using these services.

The following services are available to each learner as part of the school's online presence in *\*insert cloud service provider name\**

Using *\*insert cloud service provider name\** will enable your child to collaboratively create, edit and share files and websites for school related projects and communicate via email with other learners and members of staff. These services are entirely online and available 24/7 from any internet-connected computer.

The school believes that use of the tools significantly adds to your child's educational experience.

As the school is collecting personal data and sharing this with a third party, it should inform parents/carers about:

|                                        |                                                     |
|----------------------------------------|-----------------------------------------------------|
| This form (electronic or printed)      | The data shared with the service provider           |
| Who will have access to this form.     | What data will be shared and with whom              |
| Where this form / data will be stored. | Who will have access to the data.                   |
| How long this form will be stored for. | Where the data will be stored and for how long      |
| How this form will be destroyed.       | How a request for deletion of the data can be made. |

Do you consent to your child to having access to cloud services? Yes/No

Learner Name: .....Parent/Carers Name:.....

Signed: .....Date: .....

### Use of Biometric Systems in England and Wales

If the school uses biometric systems (e.g. fingerprint/palm recognition technologies) to identify children for access, attendance recording, charging, library lending etc it must (under the "Protection of Freedoms" and Data Protection legislation) seek permission from a parent or carer.

The school uses biometric systems for the recognition of individual children in the following ways (the school should describe here how it uses the biometric system).

Biometric technologies have certain advantages over other automatic identification systems as learners do not need to remember to bring anything with them (to the canteen or school library) so nothing can be lost, such as a swipe card.

The school has carried out a data privacy impact assessment and is confident that the use of such technologies is effective and justified in a school context.

No complete images of [fingerprints/palms](#) are stored and the original image cannot be reconstructed from the data. Meaning that it is not possible, for example, to recreate a learner's fingerprint or even the image of a fingerprint from what is in effect a string of numbers.

As the school is collecting special category personal data and *\*delete as appropriate\** sharing this with a third party, it should inform parents/carers about:

|                                             |                                                             |
|---------------------------------------------|-------------------------------------------------------------|
| This form (electronic or printed)           | The data shared with the service provider                   |
| Who will have access to this form.          | What data will be shared and with whom                      |
| Where this form / data will be stored.      | Who will have access to the data.                           |
| How long this form will be stored for.      | Where the data will be stored and for how long              |
| How this form / the data will be destroyed. | How consent to process the biometric data can be withdrawn. |

Parent/Carers Name: .....

Learner Name: .....

As the parent/carer of the above learner, I agree to the school using biometric recognition systems, as described above. Yes/No

I understand that the images cannot be used to create a whole [fingerprint/palm print](#) of my child and that these images will not be shared with anyone outside the school. Yes/No

Signed: .....

Further guidance

- (In England) Each parent of the child should be notified by the school that they are planning to process their child's biometrics and notified that they are able to object.
- In order for a school to process children's biometrics at least one parent must consent and no parent has withdrawn consent. This needs to be in writing.
- The child can object or refuse to participate in the processing of their biometric data regardless of parents' consent.
- Schools must provide reasonable alternative means of accessing services for those learners who will not be using an automated biometric recognition system.
- Permission only needs to be collected once during the period that the learner attends the school, but new permission is required if there are changes to the biometric systems in use.

### **Learner Acceptable Use Agreement**

On the following pages we have copied, for the information of parents and carers, the learner acceptable use agreement.

It is suggested that when the learner AUA is written that a copy should be attached to the parents/carers acceptable use agreement to provide information for parents and carers about the rules and behaviours that learners have committed to by signing the form.

## Appendix A5 - Staff (and Volunteer) Acceptable Use Agreement Template

Sections that include advice or guidance are written in BLUE. Schools should review and amend the contents of this agreement to ensure that it is consistent with their Online Safety Policy and other relevant school policies.

### 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 only use AI technologies approved by the school
  - will be aware of the risks of bias and discrimination, critically evaluating the outputs of AI systems for such risks
  - to protect personal and sensitive data, I will ensure that I have explicit authorisation when uploading sensitive school-related information into AI systems
  - will take care not to infringe copyright or intellectual property conventions – care will be taken to avoid intellectual property, including that of the learners, being used to train generative AI models without appropriate consent.
  - ensure that documents, emails, presentations, and other outputs influenced by AI include clear labels or notes indicating AI assistance
  - 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 Security 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 A6 - Acceptable Use Agreement for Community Users Template

**This acceptable use agreement is intended to ensure:**

- that community users of school digital technologies will be responsible users and stay safe while using these systems and devices
- that school systems, devices and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that users are protected from potential harm in their use of these systems and devices

### **Acceptable Use Agreement**

I understand that I must use school systems and devices in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems, devices and other users. This agreement will also apply to any personal devices that I bring into the school:

- I understand that my use of school systems and devices will be monitored
- I will not use a personal device that I have brought into school for any activity that would be inappropriate in a school setting.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, terrorist and extremist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.
- I will not access, copy, remove or otherwise alter any other user's files, without permission.
- I will ensure that if I take and/or publish images of others I will only do so with their permission. I will not use my personal equipment to record these images, without permission. If images are published it will not be possible to identify by name, or other personal information, those who are featured.
- I will not publish or share any information I have obtained whilst in the school on any personal website, social networking site or through any other means, unless I have permission from the school.
- I will not, without permission, make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.

- I will not install or attempt to install programmes of any type on a school device, nor will I try to alter computer settings, unless I have permission to do so.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will immediately report any damage or faults involving equipment or software, whatever the cause.
- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).
- I understand that if I fail to comply with this acceptable use agreement, the school has the right to remove my access to school systems/devices

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

As the school is collecting personal data by issuing this form, it should inform community users about:

|                                    |                                        |
|------------------------------------|----------------------------------------|
| Who will have access to this form. | How this form will be destroyed.       |
| Where this form will be stored.    | How long this form will be stored for. |

Name: ..... Signed: ..... Date: .....