Online Safety Policy Template for Sch

Grange Primary School

# Online Safety Policy



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

Version: 1

Date created: Jan 2025

Next review date: Jan 2026

## Scope of the Online Safety Policy

This Online Safety Policy outlines the commitment of Grange Primary School to safeguard members of our school community online in accordance with statutory guidance and best practice. KCSIE, [DfE Filtering and Monitoring Standards](https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges/filtering-and-monitoring-standards-for-schools-and-colleges) [DfE Cyber-Security Standards](https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges/cyber-security-standards-for-schools-and-colleges)

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

Grange Primary School will deal with such incidents within this policy, in accordance with our behaviour policy and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that take place out of school.

## Policy development, monitoring and review

4

This Online Safety Policy has been developed by the safeguarding team made up of:

* *headteacher/senior leaders*
* *Designated safeguarding lead (DSL)*
* *staff – including teachers/support staff/technical staff*
* *governors*
* *parents and carers*

## Schedule for development, monitoring and review

5

|  |  |
| --- | --- |
| This Online Safety Policy was approved by the school governing body on: |  |
| The implementation of this Online Safety Policy will be monitored by: | The Head Teacher and the DSL team |
| Monitoring will take place at regular intervals: | Termly monitoring (three times a year) |
| The *governing body* will receive a report on the implementation of the Online Safety Policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals: | Termly report (three times a year) incorporated into the Head Teachers termly report to the governors. |
| The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new technological developments, new threats to online safety or incidents that have taken place. The next anticipated review date will be: | April 2026 |
| Should serious online safety incidents take place, the following external persons/agencies should be informed: | Derbyshire Starting point 01629 533190  Police -where an illegal activity has taken place. |

## Process for monitoring the impact of the Online Safety Policy

5

The school will monitor the impact of the policy using:

* *logs of reported incidents*
* *Filtering and monitoring logs*
* *surveys/questionnaires of:*
* *learners*
* *parents and carers*
* *staff.*

# Policy and leadership

## Responsibilities

6

7

To ensure the online safeguarding of members of our school community it is important that all members of that community work together to develop safe and responsible online behaviours, learning from each other and from good practice elsewhere, reporting inappropriate online behaviours, concerns, and misuse as soon as these become apparent. While this will be a team effort, the following sections outline the online safety roles and responsibilities of individuals[[1]](#footnote-2)and groups within the school.

### Headteacher and senior leaders

* The headteacherhas a duty of care for ensuring the safety (including online safety) of members of the school community and fostering a culture of safeguarding, though the day-to-day responsibility for online safety is held by the Designated Safeguarding Lead, as defined in Keeping Children Safe in Education.
* The headteacher and (at least) another member of the senior leadership team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff[[2]](#footnote-3).
* The headteacher and deputy head teacher are responsible for ensuring that the Designated Safeguarding Lead and the safeguarding team/ IT provider/technical staff, and other relevant staff carry out their responsibilities effectively and receive suitable training to enable them to carry out their roles and train other colleagues, as relevant.
* The headteacher and deputy head teacher will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role.
* The headteacher and deputy head teacher will work with the responsible Governor, the designated safeguarding leads (DSL) and IT service providers in all aspects of filtering and monitoring.

### Governors

The DfE guidance “Keeping Children Safe in Education” states:

“Governing bodies and proprietors should ensure there are appropriate policies and procedures in place in order for appropriate action to be taken in a timely manner to safeguard and promote children’s welfare …. this includes … online safety”

“Governing bodies and proprietors should ensure an appropriate senior member of staff, from the school or college leadership team, is appointed to the role of designated safeguarding lead. The designated safeguarding lead should take lead responsibility for safeguarding and child protection (including online safety and understanding the filtering and monitoring systems and processes in place)”

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy [by asking the questions posed in the UKCIS document “Online Safety in Schools and Colleges – questions from the Governing Body”](https://www.gov.uk/government/publications/online-safety-in-schools-and-colleges-questions-from-the-governing-board).

This review will be carried out by Ashley Hobson, who will receive regular information about online safety incidents and monitoring reports. The role of Online Safety Governor will include:

* **regular meetings with the Designated Safeguarding Lead**
* **regularly receiving (collated and anonymised) reports of online safety incidents**
* **checking that provision outlined in the Online Safety Policy (e.g. online safety education provision and staff training is taking place as intended)**
* **Ensuring that** **the filtering and monitoring provision is reviewed and recorded, at least annually.**(The review will be conducted by members of the SLT, the DSL, and the IT service provider and involve the responsible governor) - in-line with the [DfE Filtering and Monitoring Standards](https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges/filtering-and-monitoring-standards-for-schools-and-colleges)
* **reporting to the full governing body**
* **Receiving (at least) basic cyber-security training to enable the governors to check that the school meets the** [**DfE Cyber-Security Standards**](https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges/cyber-security-standards-for-schools-and-colleges)

The governing body will also support the school in encouraging parents/carers and the wider community to become engaged in online safety activities.

### Designated Safety Lead (DSL)

The DSL will:

* hold the lead responsibility for online safety, within their safeguarding role.
* Receive relevant and regularly updated training in online safety to enable them to understand the risks associated with online safety and be confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online
* meet regularly with the online safety governor to discuss current issues, review (anonymised) incidents and filtering and monitoring logs and ensuring that annual (at least) filtering and monitoring checks are carried out
* attend relevant governing body meetings/groups
* report regularly to headteacher/senior leadership team
* be responsible for receiving reports of online safety incidents and handling them and deciding whether to make a referral by liaising with relevant agencies, ensuring that all incidents are recorded.
* liaise with staff and IT providers on matters of safety and safeguarding and welfare (including online and digital safety)
* have a leading role in establishing and reviewing the school online safety policies/documents
* liaise with curriculum leaders to ensure that the online safety curriculum is planned, mapped, embedded and evaluated
* ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place and the need to immediately report those incidents
* liaise with technical staff, pastoral staff and support staff (as relevant)
* receive regularly updated training to allow them to understand how digital technologies are used and are developing (particularly by learners) with regard to the areas defined In Keeping Children Safe in Education:
  + content
  + contact
  + conduct
  + commerce

### Curriculum Leads

Curriculum Leads will work with the DSL to develop a planned and coordinated online safety education programme. Grange Primary School will be using Project Evolve.

This will be provided through:

* a discrete programme of study (Project Evolve).
* PHSE curriculum modules (PSHE Matters scheme)
* A mapped cross-curricular programme
* assemblies and pastoral programmes
* through relevant national initiatives and opportunities e.g. [Safer Internet Day](https://saferinternet.org.uk/safer-internet-day/safer-internet-day-2022) and [Anti-bullying week](https://www.anti-bullyingalliance.org.uk/anti-bullying-week).

### Teaching and support staff

School staff are responsible for ensuring that:

* they have an awareness of current online safety matters/trends and of the current schoolOnline Safety Policy and practices
* they understand that online safety is a core part of safeguarding
* they have read, understood, and signed the staff acceptable use agreement (AUA)
* they follow all relevant guidance and legislation including, for example, [Keeping Children Safe in Education](https://gov.wales/keeping-learners-safe) and UK GDPR regulations
* all digital communications with learners, parents and carers and others should be on a professional level *and only carried out using official school systems and devices (where staff use AI, they should only use school-approved AI services for work purposes which have been evaluated to comply with organisational security and oversight requirements*
* they immediately report any suspected misuse or problem to the Head teacher or Deputy Head teacherfor investigation/action, in line with the school safeguarding procedures
* online safety issues are embedded in all aspects of the curriculum and other activities
* ensure learners understand and follow the Online Safety Policy and acceptable use agreements, have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
* they supervise and monitor the use of digital technologies, mobile devices, cameras, etc., in lessons and other school activities (where allowed) and implement current policies regarding these devices
* in lessons where internet use is pre-planned, learners are guided to sites checked as suitable for their use *and that processes are in place for dealing with any unsuitable material that is found in internet searches*
* where lessons take place using live-streaming or video-conferencing, there is regard to national safeguarding guidance and local safeguarding policies (n.b. the guidance contained in the [SWGfL Safe Remote Learning Resource](https://swgfl.org.uk/resources/safe-remote-learning/)
* there is a zero-tolerance approach to incidents of online-bullying, sexual harassment, discrimination, hatred etc
* they model safe, responsible, and professional online behaviours in their own use of technology, including out of school and in their use of social media.
* they adhere to the school’s technical security policy, with regard to the use of devices, systems and passwords and have an understanding of basic cybersecurity
* they have a general understanding of how the learners in their care use digital technologies out of school, in order to be aware of online safety issues that may develop from the use of those technologies
* they are aware of the benefits and risks of the use of Artificial Intelligence (AI) services in school, being transparent in how they use these services, prioritising human oversight. AI should assist, not replace, human decision-making. Staff must ensure that final judgments, particularly those affecting people, are made by humans, fact-checked and are critically evaluated.

### IT Provider

If the school has a technology service provided by an outside contractor, it is the responsibility of the school to ensure that the provider carries out all the online safety measures that the school’s obligations and responsibilities require. It is also important that the provider follows and implements school Online Safety Policy and procedures.

The IT Provider is responsible for ensuring that:

* they are aware of and follow the school Online Safety Policy and Technical Security Policy to carry out their work effectively in line with school policy
* the school technical infrastructure is secure and is not open to misuse or malicious attack
* the schoolmeets (as a minimum) the required online safety technical requirements as identified by the [DfE Meeting Digital and Technology Standards in Schools & Colleges](https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges/filtering-and-monitoring-standards-for-schools-and-colleges) and guidance from the local authority.
* there is clear, safe, and managed control of user access to networks and devices
* they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
* the use of technology is regularly and effectively monitored in order that any misuse/attempted misuse can be reported to the Head teacher or Deputy Head Teacher for investigation and action
* the filtering policy is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person.
* monitoring systems are implemented and regularly updated as agreed in school policies

### Learners

* are responsible for using the school digital technology systems in accordance with the learner acceptable use agreement and Online Safety Policy
* should understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
* should know what to do if they or someone they know feels vulnerable when using online technology.
* should avoid plagiarism and uphold copyright regulations, taking care when using Artificial Intelligence (AI) services to protect the intellectual property of themselves and others and checking the accuracy of content accessed through AI services.
* should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school’sOnline Safety Policy covers their actions out of school, if related to their membership of the school.

### Parents and carers

Parents and carers play a crucial role in ensuring that their children understand the need to use the online services and devices in an appropriate way.

The school will take every opportunity to help parents and carers understand these issues through:

* publishing the school Online Safety Policy on the school website
* providing them with a copy of the learners’ acceptable use agreement
* publish information about appropriate use of social media relating to posts concerning the school.
* seeking their permissions concerning digital images, cloud services etc
* parents’/carers’ evenings, newsletters, website, social media and information about national/local online safety campaigns and literature.

Parents and carers will be encouraged to support the school in:

* reinforcing the online safety messages provided to learners in school.

## Professional Standards

There is an expectation that professional standards will be applied to online safety as in other aspects of school life i.e.

* there is a consistent emphasis on the central importance of literacy, numeracy, digital competence and digital resilience. Learners will be supported in gaining skills across all areas of the curriculum and every opportunity will be taken to extend learners’ skills and competence
* there is a willingness to develop and apply new techniques to suit the purposes of intended learning in a structured and considered approach and to learn from the experience, while taking care to avoid risks that may be attached to the adoption of developing technologies e.g. Artificial Intelligence (AI) tools.
* Staff are able to reflect on their practice, individually and collectively, against agreed standards of effective practice and affirm and celebrate their successes
* policies and protocols are in place for the use of online communication technology between the staff and other members of the school and wider community, using officially sanctioned school mechanisms.

# Policy

11

## Online Safety Policy

The school Online Safety Policy:

* sets expectations for the safe and responsible use of digital technologies for learning, administration, and communication
* allocates responsibilities for the delivery of the policy
* is regularly reviewed in a collaborative manner, taking account of online safety incidents and changes/trends in technology and related behaviours
* establishes guidance for staff in how they should use digital technologies responsibly, protecting themselves and the school and how they should use this understanding to help safeguard learners in the digital world
* describes how the school will help prepare learners to be safe and responsible users of online technologies
* establishes clear procedures to identify, report, respond to and record the misuse of digital technologies and online safety incidents, including external support mechanisms
* is supplemented by a series of related acceptable use agreements
* is made available to staff at induction and through normal communication channels
* is published on the school website.

## Acceptable use

### Grange Primary school has defined what it regards as acceptable/unacceptable use and this is shown in the tables below.

### Acceptable use agreements

### The Online Safety Policy and acceptable use agreements define acceptable use at the school. The acceptable use agreements will be communicated/re-enforced through:

* staff induction and handbook
* communication with parents/carers
* built into education sessions
* school website
* peer support through our I-Vengers team.

| User actions 18 | | Acceptable | Acceptable at certain times | Acceptable for nominated users | Unacceptable | Unacceptable and illegal |
| --- | --- | --- | --- | --- | --- | --- |
| Users shall not access online content (including apps, games, sites) to make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to: | **Any illegal activity for example:**   * Child sexual abuse imagery\* * Child sexual abuse/exploitation/grooming * Terrorism * Encouraging or assisting suicide * Offences relating to sexual images i.e., revenge and extreme pornography * Incitement to and threats of violence * Hate crime * Public order offences - harassment and stalking * Drug-related offences * Weapons / firearms offences * Fraud and financial crime including money laundering   N.B. Schools should refer to guidance about dealing with self-generated images/sexting – [UKSIC Responding to and managing sexting incidents](https://swgfl.org.uk/assets/documents/managing-sexting-incidents.pdf?_=1554476329) and [UKCIS – Sexting in schools and colleges](https://www.gov.uk/government/publications/sexting-in-schools-and-colleges) |  |  |  |  | **✓**  **✓** |
| Users shall not undertake activities that might be classed as cyber-crime under the Computer Misuse Act (1990) | * Using another individual’s username or ID and password to access data, a program, or parts of a system that the user is not authorised to access (even if the initial access is authorised) * Gaining unauthorised access to school networks, data and files, through the use of computers/devices * Creating or propagating computer viruses or other harmful files * Revealing or publicising confidential or proprietary information (e.g., financial / personal information, databases, computer / network access codes and passwords) * Disable/Impair/Disrupt network functionality through the use of computers/devices * Using penetration testing equipment (without relevant permission)   N.B. Schools will need to decide whether these should be dealt with internally or by the police. Serious or repeat offences should be reported to the police. The National Crime Agency has a remit to prevent learners becoming involved in cyber-crime and harness their activity in positive ways– further information [here](https://www.nationalcrimeagency.gov.uk/cyber-choices) |  |  |  |  | **✓** |
| Users shall not undertake activities that are not illegal but are classed as unacceptable in school policies: | Accessing inappropriate material/activities online in a school setting including pornography, gambling, drugs. (Informed by the school’s filtering practices and/or AUAs) |  |  |  | ✓ |  |
| Promotion of any kind of discrimination |  |  |  | ✓ |  |
| Using school systems to run a private business |  |  |  | ✓ |  |
| Using systems, applications, websites or other mechanisms that bypass the filtering/monitoring or other safeguards employed by the school |  |  |  | ✓ |  |
| Infringing copyright and intellectual property (including through the use of AI services) |  |  |  | ✓ |  |
| Unfair usage (downloading/uploading large files that hinders others in their use of the internet) |  |  | ✓ | ✓ |  |
| Any other information which may be offensive to others or breaches the integrity of the ethos of the school or brings the school into disrepute |  |  |  | ✓ |  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Consideration should be given for the following activities when undertaken for non-educational purposes:  Schools may wish to add further activities to this list. | **Staff and other adults** | | | | **Learners** | | | |
| Not allowed | Allowed | Allowed at certain times | Allowed for selected staff | Not allowed | Allowed | Allowed at certain times | Allowed with staff permission/awareness |
| Online gaming on-site |  |  | ✓ |  | ✓ |  |  |  |
| Online shopping/commerce |  | ✓ |  |  | ✓ |  |  |  |
| File sharing |  | ✓ |  |  | ✓ |  |  |  |
| Social media |  |  | ✓ |  | ✓ |  |  |  |
| Messaging/chat |  |  | ✓ |  | ✓ |  |  |  |
| Entertainment streaming e.g. Netflix, Disney+ |  | ✓ |  |  | ✓ |  |  |  |
| Use of video broadcasting, e.g. YouTube, Twitch, TikTok |  |  | ✓ |  | ✓ |  |  |  |
| Mobile phones may be brought to school |  | ✓ |  |  | ✓ |  |  |  |
| Use of mobile phones for learning at school |  |  | ✓ |  | ✓ |  |  |  |
| Use of mobile phones in social time at school |  | ✓ |  |  | ✓ |  |  |  |
| Taking photos on mobile phones/cameras |  |  | ✓ | ✓ | ✓ |  |  |  |
| Use of other personal devices, e.g. tablets |  |  | ✓ | ✓ | ✓ |  |  |  |
| Use of personal e-mail in school, or on school network/wi-fi |  |  | ✓ | ✓ | ✓ |  |  |  |
| Use of school e-mail for personal e-mails | ✓ |  |  |  | ✓ |  |  |  |
| Use of AI services that have not been approved by the school |  |  | ✓ | ✓ | ✓ |  |  |  |

When using communication technologies, the school considers the following as good practice:

* when communicating in a professional capacity, staff should ensure that the technologies they use are officially sanctioned by the school.
* any digital communication between staff and learners or parents/carers (e-mail, social media, learning platform, etc.) must be professional in tone and content. *Personal e-mail addresses, text messaging or social media must not be used for these communications.*
* staff should be expected to follow good practice when using personal social media regarding their own professional reputation and that of the school and its community
* users should immediately report to a nominated person – in accordance with the school policy – the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
* relevant policies and permissions should be followed when posting information online e.g., school website and social media. Only school e-mail addresses should be used to identify members of staff and learners.

## Reporting and responding

The school will take all reasonable precautions to ensure online safety for all school users but recognises that incidents may occur inside and outside of the school (with impact on the school) which will need intervention. The school will ensure:

* there are clear reporting routes which are understood and followed by all members of the school community which are consistent with the school safeguarding procedures, and with the whistleblowing, complaints and managing allegations policies.
* all members of the school community will be made aware of the need to report online safety issues/incidents
* reports will be dealt with as soon as is practically possible once they are received
* the Designated Safeguarding Lead, Online Safety Lead and other responsible staff have appropriate skills and training to deal with online safety risks.
* if there is any suspicion that the incident involves any illegal activity or the potential for serious harm (see flowchart and user actions chart in the appendix), the incident must be escalated through the agreed school safeguarding procedures, this may include
* Non-consensual images
* Self-generated images
* Terrorism/extremism
* Hate crime/ Abuse
* Fraud and extortion
* Harassment/stalking
* Child Sexual Abuse Material (CSAM)
* Child Sexual Exploitation Grooming
* Extreme Pornography
* Sale of illegal materials/substances
* Cyber or hacking [offences under the Computer Misuse Act](https://nationalcrimeagency.gov.uk/who-we-are/publications/523-cyber-choices-hacking-it-legal-computer-misuse-act-1990/file)
* Copyright theft or piracy
* any concern about staff misuse will be reported to the Headteacher, unless the concern involves the Headteacher, in which case the complaint is referred to the Chair of Governors and the local authority
* where there is no suspected illegal activity, devices may be checked using the following procedures:
  + one or more senior members of staff should be involved in this process. This is vital to protect individuals if accusations are subsequently reported.
  + conduct the procedure using a designated device that will not be used by learners and, if necessary, can be taken off site by the police should the need arise (should illegal activity be subsequently suspected). Use the same device for the duration of the procedure.
  + ensure that the relevant staff have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
  + record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed, and attached to the form
  + once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
    - internal response or discipline procedures
    - involvement by local authority
    - police involvement and/or action
* it is important that those reporting an online safety incident have confidence that the report will be treated seriously and dealt with effectively
* there are support strategies in place e.g., peer support for those reporting or affected by an online safety incident
* incidents should be logged on MyConcern
* relevant staff are aware of external sources of support and guidance in dealing with online safety issues, e.g. local authority; police; [Professionals Online Safety Helpline](https://www.saferinternet.org.uk/helpline/professionals-online-safety-helpline); [Reporting Harmful Content](https://reportharmfulcontent.com/?lang=en); [CEOP.](http://www.ceop.police.uk/)
* those involved in the incident will be provided with feedback about the outcome of the investigation and follow up actions (as relevant)
* learning from the incident (or pattern of incidents) will be provided (as relevant and anonymously) to:
  + *the DSL and safeguarding team for consideration of updates to policies or education programmes and to review how effectively the report was dealt with*
  + *staff, through regular briefings*
  + *learners, through assemblies/lessons*
  + *parents/carers, through newsletters, school social media, website*
* *governors, through regular safeguarding updates*
* *local authority/external agencies, as relevant*

The school will make the flowchart below available to staff to support the decision-making process for dealing with online safety incidents.

Designated Safeguarding Lead (DSL) notified of an Online Safety incident1

Unsuitable or inappropriate materials or activity

Illegal materials or activities found/suspected

Convene Safeguarding Incident Review Meeting

Carry out immediate safeguarding actions necessary to protect individuals

Investigate incident and discuss with the learner / staff / to determine what happened

Update parents/carers on incident as applicable

Review policies & processes and identify learning opportunities

Ensure updates to practice are shared with staff

Implement changes and monitor situation.

Ensure the wellbeing of those involved is addressed.

Ensure Incident Log is updated and make available as required

Wellbeing of a child potentially at risk

Staff, volunteer or other adult

Follow established safeguarding arrangements and report to the Police immediately

Secure and preserve evidence in-line with Police/DOS/Safeguarding advice.

Remember, do NOT investigate yourself.

If no illegal activity or content is confirmed, revert to internal procedures

If illegal activity or content is confirmed, allow Police or relevant authority to complete their investigation and seek advice from the relevant professional body.

In the case of a member of staff or volunteer, it is possible that a suspension will take place at the point of referral to the Police whilst investigations are undertaken. Always ensure DOS advice and HR processes are correctly applied and followed

Refer to the LA, LADO and follow HR processes

Await Police response

1 This flowchart provides a suggested outline process for dealing with online safety incidents. You may wish to adapt and align with existing safeguarding policy and practice to ensure there is a consistent approach to managing safeguarding incidents in your setting.

2 The Incident Review Meeting (IRM) will typically take place as soon as possible after a serious incident to determine next steps and will usually follow any immediate safeguarding actions that have been taken (note: less serious incidents may not require an IRM).

### School actions

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

## Responding to Learner Actions

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Incidents** | Refer to class teacher | Refer to Deputy Head Teacher | Refer to Headteacher | Refer to Police/Social Work | Refer to local authority technical support for advice/action | Inform parents/carers | Remove device/ network/internet access rights | Issue a warning | Further sanction, in line with behaviour policy |
| Deliberately accessing or trying to access material that could be considered illegal (see list [in earlier section](#_User_actions) on User Actions on unsuitable/inappropriate activities). |  | ✓ | ✓ | ✓ |  | ✓ | ✓ |  | ✓ |
| Attempting to access or accessing the school network, using another user’s account (staff or learner) or allowing others to access school network by sharing username and passwords |  | ✓ | ✓ |  | ✓ | ✓ | ✓ |  | ✓ |
| Corrupting or destroying the data of other users. |  | ✓ | ✓ |  | ✓ | ✓ | ✓ |  | ✓ |
| Sending an e-mail, text or message that is regarded as offensive, harassment or of a bullying nature |  | ✓ | ✓ |  |  | ✓ | ✓ | ✓ | ✓ |
| Unauthorised downloading or uploading of files or use of file sharing. |  | ✓ | ✓ |  |  | ✓ | ✓ |  | ✓ |
| Using proxy sites or other means to subvert the school’s filtering system. |  | ✓ | ✓ |  | ✓ | ✓ | ✓ |  | ✓ |
| Accidentally accessing offensive or pornographic material and failing to report the incident. |  | ✓ | ✓ |  | ✓ | ✓ |  | ✓ |  |
| Deliberately accessing or trying to access offensive or pornographic material. |  | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |  | ✓ |
| Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act. |  | ✓ | ✓ |  |  | ✓ | ✓ | ✓ |  |
| Unauthorised use of digital devices (including taking images) |  | ✓ | ✓ |  |  | ✓ | ✓ | ✓ |  |
| Unauthorised use of online services |  | ✓ | ✓ |  |  | ✓ | ✓ | ✓ |  |
| Actions which could bring the school into disrepute or breach the integrity or the ethos of the school. |  | ✓ | ✓ |  |  | ✓ | ✓ | ✓ |  |
| Continued infringements of the above, following previous warnings or sanctions. |  | ✓ | ✓ |  |  | ✓ | ✓ |  | ✓ |

## Responding to Staff Actions

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Incidents** | Refer to line manager | Refer to Headteacher | Refer to local authority | Refer to Police | Refer to LA / Technical Support Staff for action re filtering, etc. | Issue a warning | Suspension | Disciplinary action |
| **Deliberately accessing or trying to access material that could be considered illegal (see list** [**in earlier section**](#_User_actions) **on unsuitable / inappropriate activities)** |  | ✓ | ✓ | ✓ |  |  | ✓ | ✓ |
| Actions which breach data protection or network / cyber-security rules. |  | ✓ | ✓ |  |  | ✓ |  |  |
| Deliberately accessing or trying to access offensive or pornographic material |  | ✓ | ✓ | ✓ |  |  | ✓ | ✓ |
| Corrupting or destroying the data of other users or causing deliberate damage to hardware or software |  | ✓ | ✓ | ✓ | ✓ |  |  | ✓ |
| Using proxy sites or other means to subvert the school’s filtering system. |  | ✓ | ✓ |  | ✓ | ✓ |  |  |
| Unauthorised downloading or uploading of files or file sharing |  | ✓ | ✓ |  | ✓ | ✓ |  |  |
| Breaching copyright/ intellectual property or licensing regulations (including through the use of AI systems) |  | ✓ | ✓ |  | ✓ | ✓ |  |  |
| Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person’s account. |  | ✓ | ✓ |  | ✓ | ✓ |  |  |
| Sending an e-mail, text or message that is regarded as offensive, harassment or of a bullying nature |  | ✓ | ✓ | ✓ |  | ✓ | ✓ | ✓ |
| Using personal e-mail/social networking/messaging to carry out digital communications with learners and parents/carers |  | ✓ | ✓ |  |  | ✓ |  |  |
| Inappropriate personal use of the digital technologies e.g. social media / personal e-mail |  | ✓ | ✓ |  |  | ✓ |  |  |
| Careless use of personal data, e.g. displaying, holding or transferring data in an insecure manner |  | ✓ | ✓ |  |  | ✓ |  |  |
| Actions which could compromise the staff member’s professional standing |  | ✓ | ✓ |  |  | ✓ |  |  |
| Actions which could bring the school into disrepute or breach the integrity or the ethos of the school. |  | ✓ | ✓ |  |  | ✓ |  |  |
| Failing to report incidents whether caused by deliberate or accidental actions |  | ✓ | ✓ |  |  | ✓ |  |  |
| Continued infringements of the above, following previous warnings or sanctions. |  | ✓ | ✓ |  |  | ✓ |  | ✓ |

# The use of Artificial Intelligence (AI) systems in School

As Generative Artificial Intelligence (gen AI) continues to advance and influence the world we live in, its role in education is also evolving. There are currently 3 key dimensions of AI use in schools: learner support, teacher support and school operations; ensuring all use is safe, ethical and responsible is essential.

We realise that there are risks involved in the use of Gen AI services, but that these can be mitigated through our existing policies and procedures, amending these as necessary to address the risks.

We will educate staff and learners about safe and ethical use of AI, preparing them for a future in which these technologies are likely to play an increasing role.

The safeguarding of staff and learners will, as always, be at the forefront of our policy and practice.

AI Policy Statements

* The school acknowledges the potential benefits of the use of AI in an educational context - including enhancing learning and teaching, improving outcomes, improving administrative processes, reducing workload and preparing staff and learners for a future in which AI technology will be an integral part. Staff are encouraged to use AI based tools to support their work where appropriate, within the frameworks provided below and are required to be professionally responsible and accountable for this area of their work.
* We will comply with all relevant legislation and guidance, with reference to guidance contained in Keeping Children Safe in Education and UK GDPR
* We will provide relevant training for staff and governors in the advantages, use of and potential risks of AI. We will support staff in identifying training and development needs to enable relevant opportunities.
* We will seek to embed learning about AI as appropriate in our curriculum offer, including supporting learners to understand how gen AI works, its potential benefits, risks, and ethical and social impacts. The school recognises the importance of equipping learners with the knowledge, skills and strategies to engage responsibly with AI tools.
* As set out in the staff acceptable use agreement, staff will be supported to use AI tools responsibly, ensuring the protection of both personal and sensitive data. Staff should only input anonymised data to avoid the exposure of personally identifiable or sensitive information.
* Staff will always ensure AI tools used comply with UK GDPR and other data protection regulations. They must verify that tools meet data security standards before using them for work related to the school.
* Only those AI technologies approved by the school may be used. Staff should always use school-provided AI accounts for work purposes. These accounts are configured to comply with organisational security and oversight requirements, reducing the risk of data breaches.
* We will protect sensitive information. Staff must not input sensitive information, such as internal documents or strategic plans, into third-party AI tools unless explicitly vetted for that purpose. They must always recognise and safeguard sensitive data.
* The school will ensure that when AI is used, it will not 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.
* AI incidents must be reported promptly. Staff must report any incidents involving AI misuse, data breaches, or inappropriate outputs immediately to the head teacher/deputy head teacher. Quick reporting helps mitigate risks and facilitates a prompt response.
* The school will audit all AI systems in use and assess their potential impact on staff, learners and the school’s systems and procedures, creating an AI inventory listing all tools in use, their purpose and potential risks.
* We are aware of the potential risk for discrimination and bias in the outputs from AI tools and have in place interventions and protocols to deal with any issues that may arise. When procuring and implementing AI systems, we will follow due care and diligence to prioritise fairness and safety.
* The school will support parents and carers in their understanding of the use of AI in the school.
* **Maintain Transparency in AI-Generated Content**. Staff should ensure that documents, emails, presentations, and other outputs influenced by AI include clear labels or notes indicating AI assistance. Clearly marking AI-generated content helps build trust and ensures that others are informed when AI has been used in communications or documents.
* **We will prioritise human oversight**. AI should assist, not replace, human decision-making. Staff must ensure that final judgments, particularly those affecting people, are made by humans and critically evaluate AI-generated outputs. They must ensure that all AI-generated content is fact-checked and reviewed for accuracy before sharing or publishing. This is especially important for external communication to avoid spreading misinformation.
* **Recourse for improper use and disciplinary procedures.** Improper use of AI tools, including breaches of data protection standards, misuse of sensitive information, or failure to adhere to this agreement, will be subject to disciplinary action as defined in Staff Disciplinary Policy.

## Online Safety Education Programme

While regulation and technical solutions are particularly important, their use must be balanced by educating learners to take a responsible approach. The education of learners in online safety is therefore an essential part of the school’s online safety provision. Learners need the help and support of the school to recognise and avoid online safety risks and develop their resilience.

The 2021 Ofsted “Review of Sexual Abuse in Schools and Colleges” highlighted the need for:

*“a carefully sequenced RSHE curriculum, based on the Department for Education’s (DfE’s) statutory guidance, that specifically includes sexual harassment and sexual violence, including online. This should include time for open discussion of topics that children and young people tell us they find particularly difficult, such as consent and the sending of ‘nudes’.”*

Keeping Children Safe in Education states:

“*Governing bodies and proprietors should ensure online safety is a running and interrelated theme whilst devising and implementing their whole school or college approach to safeguarding and related policies and procedures. This will include considering how online safety is reflected as required in all relevant policies and considering online safety whilst planning the curriculum …"*

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

* We will use a [planned online safety curriculum](http://www.projectevolve.co.uk/) for all year groups matched against a nationally agreed framework ([Education for a Connected Work Framework by UKCIS/DCMS](https://www.gov.uk/government/publications/education-for-a-connected-world) and the [SWGfL Project Evolve](https://projectevolve.co.uk/)) and this will be regularly taught in a variety of contexts.
* Lessons are matched to need; are age-related and build on prior learning
* Lessons are context-relevant with agreed objectives leading to clear and evidenced outcomes
* Learner need and progress are addressed through [effective planning and assessment](https://projectevolve.co.uk/guidance/knowledge-maps/)
* Digital competency is planned and effectively threaded through the appropriate digital pillars in other curriculum areas e.g. PHSE; SRE; Literacy etc
* it incorporates/makes use of relevant national initiatives and opportunities e.g. [Safer Internet Day](https://hwb.gov.wales/zones/keeping-safe-online/safer-internet-day/) and [Anti-bullying week](https://www.anti-bullyingalliance.org.uk/anti-bullying-week)
* the programme will be accessible to learners at different ages and abilities such as those with additional learning needs or those with English as an additional language.
* learners should be taught in all lessons to be critically aware of the materials/content they access online and be guided to validate the accuracy of information (including where the information is gained from Artificial Intelligence services)
* learners should be taught to acknowledge the source of information used and to respect copyright / intellectual property when using material accessed on the internet and particularly through the use of Artificial Intelligence services
* vulnerability is actively addressed as part of a personalised online safety curriculum e.g., for victims of abuse and SEND.
* learners should be helped to understand the need for the learner acceptable use agreement and encouraged to adopt safe and responsible use both within and outside school. Acceptable use is reinforced across the curriculum, with opportunities to discuss how to act within moral and legal boundaries online, with reference to the Computer Misuse Act 1990. Lessons and further resources are available on the [CyberChoices](https://www.nationalcrimeagency.gov.uk/cyber-choices) site.
* staff should act as good role models in their use of digital technologies the internet and mobile devices
* in lessons where internet use is pre-planned, it is best practice that learners should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
* where learners are allowed to freely search the internet, staff should be vigilant in supervising the learners and monitoring the content of the websites / tools (including AI systems) the learners visit
* it is accepted that from time to time, for good educational reasons, learners may need to research topics, (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff should be able to request the temporary removal of those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need
* the online safety education programme should be relevant and up to date to ensure the quality of learning and outcomes.

## Contribution of Learners

The school acknowledges, learns from, and uses the skills and knowledge of learners in the use of digital technologies. We recognise the potential for this to shape the online safety strategy for the school community and how this contributes positively to the personal development of young people. Their contribution is recognised through:

* *mechanisms to canvass learner feedback and opinion.*
* *appointment of digital leaders called ‘The I-vengers’ and the Ambassadors team (Anti-bullying).*
* *learners contribute to the online safety education programme e.g. peer education, digital leaders leading lessons for younger learners, online safety campaigns*
* *learners designing/updating acceptable use agreements*
* *contributing to online safety events with the wider school community e.g. parents’ evenings, family learning activities.*

## Staff/volunteers

All staff will receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

* a planned programme of formal online safety and data protection training will be made available to all staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.
* the training will be an integral part of the school’s annual safeguarding, data protection and cyber-security training for all staff
* all new staff will receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and acceptable use agreements. It includes explicit reference to classroom management, professional conduct, online reputation and the need to model positive online behaviours.
* the Online Safety Lead and Designated Safeguarding Lead team will receive regular updates through attendance at external training events, and by reviewing guidance documents released by relevant organisations.
* this Online Safety Policy and its updates will be presented to and discussed by staff in staff/team meetings/INSET days
* the Designated Safeguarding Lead/Online Safety Lead and the Deputy DSL will provide advice/guidance/training to individuals as required.

## Governors

Governors should take part in online safety training/awareness sessions, with particular importance for those who are members of any sub-committee/group involved in technology/online safety/health and safety/safeguarding. This may be offered in several ways such as:

* attendance at training provided by the local authority or other relevant organisation (e.g., SWGfL)
* participation in school training / information sessions for staff or parents (this may include attendance at assemblies/lessons).

A higher level of training will be made available to (at least) the Online Safety Governor. This will include:

* Cyber-security training (at least at a basic level)
* Training to allow the governor to understand the school’s filtering and monitoring provision, in order that they can participate in the required checks and reviews.

## Families

The school will seek to provide information and awareness to parents and carers through:

* regular communication, awareness-raising and engagement on online safety issues, curriculum activities and reporting routes
* regular opportunities for engagement with parents/carers on online safety issues through awareness workshops / parent/carer evenings etc
* the learners – who are encouraged to pass on to parents the online safety messages they have learned in lessons
* letters, newsletters, website,
* high profile events / campaigns e.g. [Safer Internet Day](https://www.saferinternetday.org/)
* reference to the relevant web sites/publications, e.g. [SWGfL](https://swgfl.org.uk/audience/parents/); [www.saferinternet.org.uk/](http://www.saferinternet.org.uk/); [www.childnet.com/parents-and-carers](http://www.childnet.com/parents-and-carers) (see Appendix for further links/resources).
* Sharing good practice with other schools in clusters and/or the local authority

## Adults and Agencies

The school will provide opportunities for local community groups and members of the wider community to gain from the school’s online safety knowledge and experience. This may be offered through the following:

* online safety messages targeted towards families and relatives.
* providing online safety information via their website and social media for the wider community
* supporting community groups, e.g. childminders, to enhance their online safety provision

# Technology

The school is responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. The school should ensure that all staff are made aware of policies and procedures in place on a regular basis and explain that everyone is responsible for online safety and data protection.

## Filtering & Monitoring

The school filtering and monitoring provision is agreed by senior leaders, governors and the IT Service Provider and is regularly reviewed (at least annually) and updated in response to changes in technology and patterns of online safety incidents/behaviours

Day to day management of filtering and monitoring systems requires the specialist knowledge of both safeguarding and IT staff to be effective. The DSL will have lead responsibility for safeguarding and online safety and the IT service provider will have technical responsibility

The filtering and monitoring provision is reviewed (at least annually) by senior leaders, the Designated Safeguarding Lead and a governor with the involvement of the IT Service Provider.

* checks on the filtering and monitoring system are carried out by the IT Service Provider with the involvement of a senior leader, the Designated Safeguarding Lead and a governor, in particular when a safeguarding risk is identified, there is a change in working practice, e.g. remote access or BYOD or new technology is introduced e.g. using [SWGfL Test Filtering](http://testfiltering.com/)

## Filtering

* a member of the SLT and a governor, are responsible for ensuring these standards are met.
* the school manages access to content across its systems for all users and on all devices using the school’s internet provision. The filtering provided meets the standards defined in the DfE F[iltering standards for schools and colleges](https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges/filtering-and-monitoring-standards-for-schools-and-colleges) and the guidance provided in the UK Safer Internet Centre [Appropriate filtering](https://www.saferinternet.org.uk/advice-centre/teachers-and-school-staff/appropriate-filtering-and-monitoring).
* illegal content (e.g., child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation URL list and the police assessed list of unlawful terrorist content, produced on behalf of the Home Office. Content lists are regularly updated
* there are established and effective routes for users to report inappropriate content, recognising that no system can be 100% effective. These are acted upon in a timely manner, within clearly established procedures
* there is a clear process in place to deal with, and log, requests/approvals for filtering changes
* filtering logs are regularly reviewed and alert the Designated Safeguarding Lead to breaches of the filtering policy, which are then acted upon.
* There are regular checks of the effectiveness of the filtering systems . Checks are undertaken across a range of devices at least termly and the results recorded and analysed to inform and improve provision. The DSL and Governor are involved in the process and aware of the findings. (Schools may wish to use e.g. using SWGfL Testfiltering.com to carry out these checks)
* Devices that are provided by the school have school-based filtering applied irrespective of their location.
* younger learners will use child friendly/age-appropriate search engines e.g. [SWGfL Swiggle](https://swiggle.org.uk/)
* the school has a mobile phone policy and where personal mobile devices have internet access through the school network, content is managed in ways that are consistent with school policy and practice.
* access to content through non-browser services (e.g. apps and other mobile technologies) is managed in ways that are consistent with school policy and practice.

If necessary, the school will seek advice from, and report issues to, the SWGfL [Report Harmful Content](https://hwb.gov.wales/news/articles/0165ae84-0055-49b4-9bf2-0aedc29c5582) site.

## Monitoring

The school follows the UK Safer Internet Centre [Appropriate Monitoring](https://www.saferinternet.org.uk/advice-centre/teachers-and-school-staff/appropriate-filtering-and-monitoring) guidance.

The school has monitoring systems in place, agreed by senior leaders and technical staff, to protect the school, systems and users:

* The school monitors all network use across all its devices and services.
* monitoring reports are urgently picked up, acted on and outcomes are recorded by the Designated Safeguarding Lead, all users are aware that monitoring is in place.
* There are effective protocols in place to report abuse/misuse. There is a clear process for prioritising response to alerts that require rapid safeguarding intervention.
* Management of serious safeguarding alerts is consistent with safeguarding policy and practice.
* The monitoring provision is reviewed at least once every academic year and updated in response to changes in technology and patterns of online safety incidents and behaviours. The review should be conducted by members of thesenior leadershipteam, the designated safeguarding lead, and technical staff. It will also involve the responsible governor. The results of the review will be recorded and reported as relevant.
* Devices that are provided by the school have school-based monitoring applied irrespective of their location.
* monitoring enables alerts to be matched to users and devices.

## Technical Security

The school technical systems will be managed in ways that ensure that the school meets recommended standards in the [DfE Technical Standards for Schools and Colleges](https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges/filtering-and-monitoring-standards-for-schools-and-colleges)

* responsibility for technical security resides with SLT who may delegate activities to identified roles.
* A documented access control model is in place, clearly defining access rights to school systems and devices. This is reviewed annually. All users (staff and learners) have responsibility for the security of their username and password and must not allow other users to access the systems using their log on details. Users must immediately report any suspicion or evidence that there has been a breach of security
* password policy and procedures are implemented and are consistent with guidance from the National Cyber Security Centre
* all school networks, devices and system will be protected by secure passwords.
* the administrator passwords for school systems are kept in a secure place, e.g. school safe.
* there is a risk-based approach to the allocation of learner usernames and passwords.
* there will be regular reviews and audits of the safety and security of school technical systems
* servers, wireless systems and cabling are securely located and physical access restricted
* appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems and devices from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up-to-date endpoint software.
* there are rigorous and verified back-up routines, including the keeping of network-separated (air-gapped) copies off-site or in the cloud,
* The business manager is responsible for ensuring that all software purchased by and used by the school is adequately licenced and that the latest software updates (patches) are applied.
* an appropriate system is in place for users to report any actual/potential technical incident/security breach to the relevant person, as agreed.
* use of school devices out of school and by family members is regulated by an acceptable use statement that a user consents to when the device is allocated to them
* personal use of any device on the school network is regulated by acceptable use statements that a user consents to when using the network
* staff members are not permitted to install software on a school-owned devices without the consent of the SLT/IT service provider
* removable media is not permitted unless approved by the SLT/IT service provider
* systems are in place to control and protect personal data and data is encrypted at rest and in transit.
* guest users are provided with appropriate access to school systems based on an identified risk profile.
* systems are in place that prevent the unauthorised sharing of personal / sensitive data unless safely encrypted or otherwise secured.
* Care will be taken when using Artificial Intelligence services to avoid the input of sensitive information, such as personal data, internal documents or strategic plans, into third-party AI systems unless explicitly vetted for that purpose. Staff must always recognise and safeguard sensitive data.
* dual-factor authentication is used for sensitive data or access outside of a trusted network
* Where AI services are used, the school will work with suppliers to understand how these services are trained and will regularly review flagged incidents to ensure equality for all users e.g. avoiding bias

## Mobile technologies

At Grange Primary School, learners are not allowed the use of mobile phones during the school day. If learners need to bring their mobile phones to school for reasons that include:

* Safety to and from home/school
* Transition from one family home to another at the beginning/end of a school day

learners are instructed to switch their mobile phones off at the school gates and hand them in to class teachers on arrival for secure storage. Mobile phones are handed back to learners at the end of the school day and can only be switched on after leaving the school premises.

Smart watches or any other device that connects to the internet are also included in these procedures.

The school acceptable use agreements for staff, learners, parents, and carers outline the expectations around the use of mobile technologies.

Grange Primary School does not hold any liability for loss/damage or malfunction of personal devices that are brought into school and are/are not stored securely during the day. If learners do not hand in mobile devices for secure storage at the beginning of the day, the behaviour policy will be followed.

Education about the safe and responsible use of mobile devices is included in the school online safety education programmes.

**For staff,** the use of personal devices for school business is defined in the acceptable use policy and staff handbook.

Staff are not permitted to use their mobile devices during the school day unless it is in a ‘child free zone’. The use of mobile devices should be limited to break times or lunch times unless pre-agreed by the head teacher/deputy head teacher for a specific purpose.

Staff are not permitted to take images on their mobile phones that link to school learners unless pre-agreed by the head teacher/deputy head teacher for a specific purpose, and that these images are safely and swiftly transferred onto secure school systems for storage and permanently deleted from any mobile device. Staff do not take any pre-agreed images without the attendance of another member of staff.

The purpose of any pre-agreed images/videos may include content for the school website that requires a high spec of technology, or evidence of learner’s experiences on school trips and residentials where the use of school based technology cannot be achieved.

The non-consensual taking/using of images of others is not permitted.

**School visitors** are made aware of our mobile device policy on arrival and, if they are not office based and will be working with learners without the supervision of a member of the Grange Primary School staff, are asked to store these securely in the office area.

## Social media

Expectations for teachers’ professional conduct are set out in the [DfE Teachers Standards](https://www.gov.uk/government/publications/teachers-standards) but all adults working with children and young people must understand that the nature and responsibilities of their work place them in a position of trust and that their conduct should reflect this.

All schools and local authorities have a duty of care to provide a safe learning environment for learners and staff. Schools could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, bully online, discriminate on the grounds of sex, race, or disability or who defame a third party may render the school liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to learners through:

* ensuring that personal information is not published.
* education/training is provided that includes acceptable use, age restrictions, social media risks, digital and video images policy, checking of settings, data protection and reporting issues.
* clear reporting guidance, including responsibilities, procedures, and sanctions.
* risk assessment, including legal risk.
* guidance for learners, parents/carers

School staff should ensure that:

* No reference should be made in social media to learners, parents/carers or school staff.
* they do not engage in online discussion on personal matters relating to members of the school community.
* personal opinions should not be attributed to the school.
* security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.
* they act as positive role models in their use of social media

When official school social media accounts are established, there should be:

* a process for approval by senior leaders
* clear processes for the administration, moderation, and monitoring of these accounts – involving at least two members of staff
* a code of behaviour for users of the accounts
* systems for reporting and dealing with abuse and misuse
* understanding of how incidents may be dealt with under school disciplinary procedures.

### Personal use

* personal communications are those made via personal social media accounts. In all cases, where a personal account is used which associates itself with, or impacts on, the school it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy
* personal communications which do not refer to or impact upon the school are outside the scope of this policy
* where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
* the school permits reasonable and appropriate access to personal social media sites during school hours

### Monitoring of public social media

* As part of active social media engagement, the school may pro-actively monitor the Internet for public postings about the school.
* the school should effectively respond to social media comments made by others according to a defined policy or process.
* when parents/carers express concerns about the school on social media we will urge them to make direct contact with the school, in private, to resolve the matter. Where this cannot be resolved, parents/carers should be informed of the school complaints procedure.

## Digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and learners instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and learners need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for online bullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees.

The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

* the school may use live-streaming or video-conferencing services in line with national and local safeguarding guidance / policies. Guidance can be found on the [SWGfL Safer Remote Learnin](https://swgfl.org.uk/resources/safe-remote-learning/)g web pages and in the [DfE Safeguarding and remote education](https://www.gov.uk/guidance/safeguarding-and-remote-education-during-coronavirus-covid-19).
* when using digital images, staff will inform and educate learners about the risks associated with the taking, use, sharing, publication and distribution of images.
* staff/volunteers must be aware of those learners whose images must not be taken/published. Those images should only be taken on school devices. The personal devices of staff should not be used for those such purposes.
* in accordance with [guidance from the Information Commissioner’s Office](https://ico.org.uk/for-organisations/sme-web-hub/whats-new/blogs/taking-photographs-data-protection-advice-for-schools/), parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone’s privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other learners in the digital/video images
* staff and volunteers are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, storage, distribution and publication of those images
* care should be taken when sharing digital/video images that learners are appropriately dressed
* learners must not take, use, share, publish or distribute images of others without their permission
* photographs published on the website, or elsewhere that include learners will be selected carefully and will comply with Online Safety Policy
* learners’ full names will not be used anywhere on a website or blog, particularly in association with photographs.
* written permission from parents or carers will be obtained before photographs of learners are taken for use in school or published on the school website/social media.Permission is not required for images taken solely for internal purposes.
* parents/carers will be informed of the purposes for the use of images, how they will be stored and for how long – in line with the school data protection policy
* images will be securely stored in line with the school retention policy
* learners’ work can only be published with the permission of the learner and parents/carers.

## Online Publishing

The school communicates with parents/carers and the wider community and promotes the school through:

* Public-facing website
* Newsletters sent via WEDUC which are also published on the school’s website.

The school website hosted by Juniper Education.org and is managed and monitored by the head teacher and deputy head teacher. The school ensures that the online safety policy has been followed in the use of online publishing e.g., use of digital and video images, copyright, identification of young people, publication of school calendars and personal information – ensuring that there is least risk to members of the school community, through such publications.

Where learner work, images or videos are published, their identities are protected, and full names are not published.

The school public online publishing provides information about online safety e.g., publishing the schools Online Safety Policy and acceptable use agreements; curating latest advice and guidance; news articles etc, creating an online safety page on the school website.

The website includes an online reporting process for parents and the wider community to register issues and concerns to complement the internal reporting process.

## Data Protection

Personal data will be recorded, processed, transferred, and made available according to the current data protection legislation.

The school:

* **has a Data Protection Policy.**
* **implements the data protection principles and can demonstrate that it does so**
* **has paid the appropriate fee to the Information Commissioner’s Office (ICO)**
* **has appointed an appropriate Data Protection Officer (DPO) who has effective understanding of data protection law and is free from any conflict of interest. Grange Primary School use the Derbyshire Data protection for school service.**
* **has a ‘Record of Processing Activities’ in place and knows exactly what personal data is held, where, why and which member of staff has responsibility for managing it**
* **the Record of Processing Activities lists the lawful basis for processing personal data (including, where relevant, consent). Where special category data is processed, an additional lawful basis is listed**
* **has an ‘information asset register’ in place and knows exactly** [**what personal data is held**](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/what-is-personal-data/what-is-personal-data/)**, where, why and which member of staff has responsibility for managing it**
* **information asset register lists the lawful basis for processing personal data (including, where relevant, consent). Where special category data is processed, an additional lawful basis will have also been listed**
* **will hold the minimum personal data necessary to enable it to perform its function and will not hold it for longer than necessary for the purposes it was collected for. The school ‘retention schedule” supports this**
* **data held is accurate and up to date and is held only for the purpose it was held for. Systems are in place to identify inaccuracies, such as asking parents to check emergency contact details at suitable intervals**
* **provides staff, parents, volunteers, teenagers, and older children with information about how the school looks after their data and what their rights are in a clear Privacy Notice** (see Privacy Notice section in the appendix)
* **has procedures in place to deal with the individual rights of the data subject,** e.g. one of the dozen rights applicable is that of Subject Access which enables an individual to see/have a copy of the personal data held about them
* **carries out Data Protection Impact Assessments (DPIA) where necessary e.g. to ensure protection of personal data when accessed using any remote access solutions, or entering into a relationship with a new supplier**
* **has undertaken appropriate due diligence and has data protection compliant contracts in place with any data processors**
* **understands how to share data lawfully and safely with other relevant data controllers.**
* **has clear and understood policies and routines for the deletion and disposal of data**
* [**reports any relevant breaches to the Information Commissioner**](https://ico.org.uk/for-organisations/report-a-breach/) **within 72hrs of becoming aware of the breach as required by law. It also reports relevant breaches to the individuals affected as required by law. In order to do this, it has a policy for reporting, logging, managing, investigating and learning from information risk incidents**
* **has a Freedom of Information Policy which sets out how it will deal with FOI requests**
* **provides data protection training for all staff at induction and appropriate refresher training thereafter. Staff undertaking particular data protection functions, such as handling requests under the individual’s rights, will receive training appropriate for their function as well as the core training provided to all staff**
* ensures that where AI services are used, data privacy is prioritised

When personal data is stored on any mobile device or removable media the:

* **data will be encrypted, and password protected.**
* **device will be password protected**.
* **device will be protected by up-to-date endpoint (anti-virus) software**

16

* **data will be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete.**

Staff must ensure that they:

* **at all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse**
* **can recognise a possible breach, understand the need for urgency and know who to report it to within the school**
* **can help data subjects understand their rights and know how to handle a request whether verbal or written and know who to pass it to in the school**
* **only use encrypted data storage for personal data**
* **will not transfer any school personal data to personal devices. School laptops are provided for working at home and ‘Foldr’ (a secure cloud-based system) is used to securely access school documents from site based servers.**
* **use personal data only on secure password protected computers and other devices, ensuring that they are properly “logged-off” at the end of any session in which they are using personal data**
* **transfer data using encryption, a secure email account (where appropriate), and secure password protected devices.**

## Cyber Security (new January 2025)

[The DfE Cyber security standards for schools and colleges explains:](https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges/cyber-security-standards-for-schools-and-colleges)

“Cyber incidents and attacks have significant operational and financial impacts on schools and colleges. These incidents or attacks will often be an intentional and unauthorised attempt to access, change or damage data and digital technology. They could be made by a person, group, or organisation outside or inside the school or college and can lead to:

* safeguarding issues due to sensitive personal data being compromised
* impact on student outcomes
* a significant data breach
* significant and lasting disruption, including the risk of repeated future cyber incidents and attacks, including school or college closure
* financial loss
* reputational damage”

The [‘Cyber-security in schools: questions for governing bodies and Trustees’](https://www.ncsc.gov.uk/information/school-governor-questions) guidance produced by the National Cyber Security Centre (NCSC) aims to support governing bodies’ and management committees’ understanding of their education settings’ cyber security risks. The guidance includes eight questions to facilitate the cyber security conversation between the governing body and school leaders, with the governing body taking the lead.

* the school has reviewed the DfE Cyber security standards for schools and colleges and is working toward meeting these standards
* the school will conduct a cyber risk assessment annually and review each term
* the school, (*in partnership with their technology support partner),* has identified the most critical parts of the school’s digital and technology services and sought assurance about their cyber security
* the school has an effective backup and restoration plan in place in the event of cyber attacks
* the school’s governance and IT policies reflect the importance of good cyber security
* staff and Governors receive training on the common cyber security threats and incidents that schools experience
* the school’s education programmes include cyber awareness for learners
* the school has a business continuity and incident management plan in place
* there are processes in place for the reporting of cyber incidents. All students and staff have a responsibility to report cyber risk or a potential incident or attack, understand how to do this and feel safe and comfortable to do so.

# Outcomes

The impact of the Online Safety Policy and practice is regularly evaluated through the review/audit of online safety incident logs; behaviour/bullying reports; surveys of staff, learners; parents/carers and is reported to relevant groups:

* there is balanced professional debate about the evidence taken from the reviews/audits and the impact of preventative work e.g., online safety education, awareness, and training
* there are well-established routes to regularly report patterns of online safety incidents and outcomes to school leadership and Governors
* parents/carers are informed of patterns of online safety incidents as part of the school’s online safety awareness raising
* online safety (and related) policies and procedures are regularly updated in response to the evidence gathered from these reviews/audits/professional debate
* the evidence of impact is shared with other schools, agencies and LAs to help ensure the development of a consistent and effective local online safety strategy.

This policy will be reviewed in April 2026.

# 

# Grange Primary School Online Safety Policy Appendices

# Appendices

A1 - Learner Acceptable Use Agreement Template – KS2

A2 - Learner Acceptable Use Agreement Template – for younger learners (Foundation/KS1)

A3 - Parent/Carer Acceptable Use Agreement Template

A4 - Staff (and Volunteer) Acceptable Use Policy Agreement Template

A5 - Community Users Acceptable Use Agreement Template

A6 - Computer misuse and cyber choices policy

A7 – Responding to incidents of misuse – flowchart.

A8 - Record of reviewing devices/internet sites (responding to incidents of misuse)

A9 - Reporting Log

B1 - Training Needs Audit Log

C1 – Legislation

C2 - Links to other organisations and resources

C3 - Glossary of Terms

# **Appendix A1 - Learner Acceptable Use Agreement – for KS2**

### 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 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:

# **A2 Learner Acceptable Use Agreement – for younger learners (Early Years/KS1)**

**Our Technology Rules**

I will follow these rules to use computers, tablets and the internet safely 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.

These rules help us all stay safe and have fun using computers and tablets at school!

Signed (child):

Signed (parent):

# A3 Parent/Carer Acceptable Use Agreement

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.

Grange Primary 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 available on our on-line safety page on our website so that parents/carers will be aware of the school expectations of the young people in their care.

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

### Permission Form

Parent/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 know that my son/daughter has signed an acceptable use agreement and has 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.

**Or: (KS1)**

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 mobile technologies.

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 the internet and digital technologies at home and will inform the school if I have concerns over my child’s online safety.

This form will be stored securely in the head teacher’s office and will be destroyed as your child leaves Grange Primary School or if there is an updated agreement that replaces it.

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 use digital cameras to record evidence of activities in lessons. These images may then be used in presentations in subsequent lessons and will be for internal use only.

Images may also be used to celebrate success through their publication in newsletters, on the school website and occasionally in the public media. Where you have given permission for your child’s image to be used publicly (on our permissions forms), only your child’s first name will be used.

The school complies with the Data Protection Act by requesting parent’s/carer’s permission before taking images of members of the school. This form is filled in when your child starts Grange Primary School, and we would like to update that information today using the form below. 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 Grange Primary school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone’s privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other learners in the digital/video images.

Parents/carers are requested to sign the permission form below to allow Grange Primary School to take and use images of their children and for the parents/carers to agree.

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: |  |
| * to support learning activities internally in school. | Yes/No |
| * in publicity that reasonably celebrates success and promotes the work of the school e.g on the school’s website, school newsletters | Yes/No |
| * in publicity that is used by external agencies, such as newspapers | 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:

This printed form will be accessible to relevant school staff and will be stored securely in the school office. This form will be kept for the duration of your child’s time at Grange Primary School and will be deleted in a safe way as your child leaves Grange Primary School.

Any images of your child will be stored on the school’s secure server and will only be accessible to relevant school staff. These images may be published on the school website permissions accepting. Images of your child will be electronically deleted from the secure server within 6 months of your child leaving Grange Primary School. A request for the deletion of these images can be made in writing to the Head teacher.

# A4 Staff (and Volunteer) Acceptable Use Agreement

### 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.

28

* 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 the internet 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 a warning, a suspension, referral to Governors and/or the Local Authority 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:

# A5 Acceptable Use Agreement for Community Users

### 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.e the head teacher

28

* 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.

This form will be accessed by the Head teacher and will be stored securely in the head teacher’s office. This form will be stored for the duration of your working relationship with the school and will be destroyed two years after your work has been completed.

Name: Signed: Date: …………………………………….

# A6 Computer Misuse and Cyber Choices Policy

All key stakeholders, including the school IT service provider, have responsibility for the safeguarding of young people from computer misuse and are aware of the Cyber Choices programme led by the National Crime Agency (NCA) and managed locally by Regional Organised Crime Units (part of the national policing network).  The risks to young people of crossing the line into committing cybercrimes is a safeguarding issue. This often happens without the individual even realising, young people need support in making the right #CyberChoices in their use of technology. Young people with an interest in technology, a high IQ, and an appetite to engage in risky behaviours are considered to be at a higher risk of committing a cyber offence, but many first-time offenders are also unaware of what the law governing cyber offences actually is. The average age of first-time cyber offenders in the UK has fallen significantly in recent years. The Cyber Choices programme works with individuals committing, or at risk of committing, cybercrimes which can only be carried out with technology, where devices are both the tool for committing the crime, and the target of the crime.

All staff are made aware of the safeguarding risks of computer misuse.

All staff are familiar with the [NCA Hacking it Legal Leaflet](https://nationalcrimeagency.gov.uk/who-we-are/publications/526-cyber-choices-hacking-it-legal-teachers/file)\*, which explains Cyber Choices and the Computer Misuse Act 1990, and lists recommended resources for teachers to use.

Staff are aware of the role of their local Regional Organised Crime Unit as their point of contact for Cyber Choices referrals.

Learners agree to the Acceptable Use Policy (AUP) which outlines acceptable online behaviours and explains that some online activity is illegal. Acceptable computer use is reinforced across the curriculum, with opportunities to discuss how to act within moral and legal boundaries online, with reference to the Computer Misuse Act 1990. Lessons and further resources are available on the NCA [Cyber Choices](https://www.nationalcrimeagency.gov.uk/cyber-choices) site.

Any breach of the AUP or activity by a learner that may constitute a cybercrime, in school or at home, will be referred to the Designated Safeguarding Lead for consideration as a safeguarding risk.

Where the DSL believes that the learner may be at risk of committing cybercrimes, or to already be committing cybercrimes, a referral to the local [Cyber Choices](https://www.nationalcrimeagency.gov.uk/cyber-choices) programme will be made (contact details for all Regional Organised Crime Units are available in the “what to do if you’re concerned” section at the bottom of the [NCA Cyber Choices page).](https://www.nationalcrimeagency.gov.uk/cyber-choices) Where the DSL is unsure if a learner meets the referral criteria, advice should be sought from the local Cyber Choices team.

Parents also have the opportunity to report potential cybercrime directly to the local Cyber Choices team but are recommended to make school-based concerns through the DSL who is the head teacher at Grange Primary School.

The IT service provider is aware of the safeguarding requirement to refer concerns about computer misuse to the Designated Safeguarding Lead and has a clear process to follow in order to do so.

Information for parents about NCA Cyber Choices is available on the school website.

*This policy template is based on a document for schools published by the South East Regional Organised Crime Unit (SEROCU) and has been amended for use across the UK. SWGfL would like to acknowledge the support of SEROCU for permission to adapt and use the document.*

# A7 Responding to incidents of misuse – flow chart

Designated Safeguarding Lead (DSL) notified of an Online Safety incident1

Unsuitable or inappropriate materials or activity

Illegal materials or activities found/suspected

Convene Safeguarding Incident Review Meeting

Carry out immediate safeguarding actions necessary to protect individuals

Investigate incident and discuss with the learner / staff / to determine what happened

Update parents/carers on incident as applicable

Review policies & processes and identify learning opportunities

Ensure updates to practice are shared with staff

Implement changes and monitor situation.

Ensure the wellbeing of those involved is addressed.

Ensure Incident Log is updated and make available as required

Wellbeing of a child potentially at risk

Staff, volunteer or other adult

Follow established safeguarding arrangements and report to the Police immediately

Secure and preserve evidence in-line with Police/DOS/Safeguarding advice.

Remember, do NOT investigate yourself.

If no illegal activity or content is confirmed, revert to internal procedures

If illegal activity or content is confirmed, allow Police or relevant authority to complete their investigation and seek advice from the relevant professional body.

In the case of a member of staff or volunteer, it is possible that a suspension will take place at the point of referral to the Police whilst investigations are undertaken. Always ensure DOS advice and HR processes are correctly applied and followed

Refer to the LA, LADO and follow HR processes

Await Police response

1 This flowchart provides a suggested outline process for dealing with online safety incidents. You may wish to adapt and align with existing safeguarding policy and practice to ensure there is a consistent approach to managing safeguarding incidents in your setting.

2 The Incident Review Meeting (IRM) will typically take place as soon as possible after a serious incident to determine next steps and will usually follow any immediate safeguarding actions that have been taken (note: less serious incidents may not require an IRM).

# A8 Record of reviewing devices/internet sites (responding to incidents of misuse)

Group:

Date:

Reason for investigation:

#### Details of first reviewing person

Name:

Position:

Signature:

#### Details of second reviewing person

Name:

Position:

Signature:

#### Name and location of computer used for review (for web sites)

|  |  |
| --- | --- |
| Web site(s) address/device | Reason for concern |
|  |  |
|  |  |
|  |  |

#### Conclusion and Action proposed or taken

|  |  |
| --- | --- |
|  |  |
|  |  |
|  |  |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| A9 Reporting Log Group: | | | | | | | | | |
| Date | Time | Incident | | Action Taken | | | Incident Reported By | | Signature |
| What? | | By Whom? |
|  |  |  | |  | |  |  | |  |
|  |  |  | |  | |  |  | |  |
|  |  |  | |  | |  |  | |  |
|  |  |  | |  | |  |  | |  |
|  |  |  | |  | |  |  | |  |
|  |  |  | |  | |  |  | |  |
| B1 Training Needs Audit Log Group: | | | | | | | | | |
| Relevant training the last 12 months | | | Identified Training Need | | To be met by | | | Cost | Review Date |
|  | | |  | |  | | |  |  |
|  | | |  | |  | | |  |  |
|  | | |  | |  | | |  |  |
|  | | |  | |  | | |  |  |
|  | | |  | |  | | |  |  |
|  | | |  | |  | | |  |  |

**C1 Legislation**

All school stakeholders should be aware of the legislative framework under which this online safety policy has been produced. It is important to note that in general terms an action that is illegal if committed offline is also illegal if committed online.

It is recommended that legal advice is sought in the advent of an online safety issue or situation.

A useful summary of relevant legislation can be found at: [Report Harmful Content: Laws about harmful behaviours](https://reportharmfulcontent.com/when-should-you-go-to-the-police/)

### Computer Misuse Act 1990

This Act makes it an offence to:

* Erase or amend data or programs without authority;
* Obtain unauthorised access to a computer;
* “Eavesdrop” on a computer;
* Make unauthorised use of computer time or facilities;
* Maliciously corrupt or erase data or programs;
* Deny access to authorised users.

Schools may wish to view the National Crime Agency website which includes information about [“Cyber crime – preventing young people from getting involved”](https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/cyber-crime/cyber-crime-preventing-young-people-from-getting-involved). Each region in England (& Wales) has a Regional Organised Crime Unit (ROCU) Cyber-Prevent team that works with schools to encourage young people to make positive use of their cyber skills. There is a useful [summary of the Act on the NCA site](https://nationalcrimeagency.gov.uk/who-we-are/publications/75-guide-to-the-computer-misuse-act/file).

### Data Protection Act 1998

This protects the rights and privacy of individual’s data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Act states that person data must be:

* Fairly and lawfully processed.
* Processed for limited purposes.
* Adequate, relevant and not excessive.
* Accurate.
* Not kept longer than necessary.
* Processed in accordance with the data subject’s rights.
* Secure.
* Not transferred to other countries without adequate protection.

### The Data Protection Act 2018:

#### Updates the 1998 Act, incorporates the General Data Protection Regulations (GDPR) and aims to:

* Facilitate the secure transfer of information within the European Union.
* Prevent people or organisations from holding and using inaccurate information on individuals. This applies to information regarding both private lives or business.
* Give the public confidence about how businesses can use their personal information.
* Provide data subjects with the legal right to check the information businesses hold about them. They can also request for the data controller to destroy it.
* Give data subjects greater control over how data controllers handle their data.
* Place emphasis on accountability. This requires businesses to have processes in place that demonstrate how they’re securely handling data.
* Require firms to keep people’s personal data safe and secure. Data controllers must ensure that it is not misused.
* Require the data user or holder to register with the Information Commissioner.

#### All data subjects have the right to:

* Receive clear information about what you will use their data for.
* Access their own personal information.
* Request for their data to be revised if out of date or erased. These are known as the right to rectification and the right to erasure
* Request information about the reasoning behind any automated decisions, such as if computer software denies them access to a loan.
* Prevent or query about the automated processing of their personal data.

### Freedom of Information Act 2000

The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures.

### Communications Act 2003

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

### Malicious Communications Act 1988

It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.

### Regulation of Investigatory Powers Act 2000

It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to:

* Establish the facts;
* Ascertain compliance with regulatory or self-regulatory practices or procedures;
* Demonstrate standards, which are or ought to be achieved by persons using the system;
* Investigate or detect unauthorised use of the communications system;
* Prevent or detect crime or in the interests of national security;
* Ensure the effective operation of the system.
* Monitoring but not recording is also permissible in order to:
* Ascertain whether the communication is business or personal;
* Protect or support help line staff.
* The school reserves the right to monitor its systems and communications in line with its rights under this act.

### Trade Marks Act 1994

This provides protection for Registered Trade Marks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trade Marks must not be used without permission. This can also arise from using a Mark that is confusingly similar to an existing Mark.

### Copyright, Designs and Patents Act 1988

It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. YouTube).

### Telecommunications Act 1984

It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

### Criminal Justice & Public Order Act 1994

This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they:

* Use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or
* Display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

### Racial and Religious Hatred Act 2006

This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

### Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

### Protection of Children Act 1978

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison

### Sexual Offences Act 2003

A grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

### Public Order Act 1986

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence. Children, Families and Education Directorate page 38 April 2007.

### Obscene Publications Act 1959 and 1964

Publishing an “obscene” article is a criminal offence. Publishing includes electronic transmission.

### Human Rights Act 1998

This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of “higher law”, affecting all other laws. In the school context, human rights to be aware of include:

* The right to a fair trial
* The right to respect for private and family life, home and correspondence
* Freedom of thought, conscience and religion
* Freedom of expression
* Freedom of assembly
* Prohibition of discrimination
* The right to education

These rights are not absolute. The school is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.

### The Education and Inspections Act 2006

Empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of learners when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.

51

### The Education and Inspections Act 2011

Extended the powers included in the 2006 Act and gave permission for Headteachers (and nominated staff) to search for electronic devices. It also provides powers to search for data on those devices and to delete data.

(see template policy in these appendices and for DfE guidance - [http://www.education.gov.uk/schools/learnersupport/behaviour/behaviourpolicies/f0076897/screening-searching-and-confiscation](http://www.education.gov.uk/schools/pupilsupport/behaviour/behaviourpolicies/f0076897/screening-searching-and-confiscation))

### The Protection of Freedoms Act 2012

Requires schools to seek permission from a parent/carer to use Biometric systems

### The School Information Regulations 2012

Requires schools to publish certain information on its website:

<https://www.gov.uk/guidance/what-maintained-schools-must-publish-online>

### Serious Crime Act 2015

Introduced new offence of sexual communication with a child. Also created new offences and orders around gang crime (including CSE)

### Criminal Justice and Courts Act 2015

Revenge porn – as it is now commonly known – involves the distribution of private and personal explicit images or video footage of an individual without their consent, with the intention of causing them embarrassment and distress. Often revenge porn is used maliciously to shame ex-partners. Revenge porn was made a specific offence in the Criminal Justice and Courts Act 2015. The Act specifies that if you are accused of revenge porn and found guilty of the criminal offence, you could be prosecuted and face a sentence of up to two years in prison.

For further guidance or support please contact the [Revenge Porn Helpline](https://revengepornhelpline.org.uk/)

## C2 Links to other organisations or documents

### UK Safer Internet Centre

Safer Internet Centre – <https://www.saferinternet.org.uk/>

South West Grid for Learning - h[ttps://swgfl.org.uk/products-services/online-safety/](http://www.swgfl.org.uk/)

Childnet – <http://www.childnet-int.org/>

Professionals Online Safety Helpline - <http://www.saferinternet.org.uk/about/helpline>

Revenge Porn Helpline - https://revengepornhelpline.org.uk/

Internet Watch Foundation - <https://www.iwf.org.uk/>

Report Harmful Content - <https://reportharmfulcontent.com/>

Harmful Sexual [Support](https://swgfl.org.uk/harmful-sexual-behaviour-support-service/) Service

### CEOP

CEOP - <http://ceop.police.uk/>

[ThinkUKnow](http://www.thinkuknow.co.uk/) - <https://www.thinkuknow.co.uk/>

### Others

[LGfL – Online Safety Resources](https://www.lgfl.net/online-safety/resource-centre?a=3)

[Kent – Online Safety Resources page](http://www.kelsi.org.uk/child-protection-and-safeguarding/e-safety/e-safety-classroom-materials)

INSAFE/Better Internet for Kids - <https://www.betterinternetforkids.eu/>

UK Council for Internet Safety (UKCIS) - <https://www.gov.uk/government/organisations/uk-council-for-internet-safety>

### Tools for Schools / other organisations

Online Safety BOOST – <https://boost.swgfl.org.uk/>

360 Degree Safe – Online Safety self-review tool – <https://360safe.org.uk/>

360Data – online data protection self-review tool: [www.360data.org.uk](http://www.360data.org.uk/)

SWGfL Test filtering - <http://testfiltering.com/>

UKCIS Digital Resilience Framework - <https://www.gov.uk/government/publications/digital-resilience-framework>

[SWGfL 360 Groups](http://www.360groups.org.uk/) – online safety self review tool for organisations working with children

[SWGfL 360 Early Years](http://www.360earlyyears.org.uk/) - online safety self review tool for early years organisations

### Bullying/Online-bullying/Sexting/Sexual Harassment

Enable – European Anti Bullying programme and resources (UK coordination/participation through SWGfL & Diana Awards) - <http://enable.eun.org/>

SELMA – Hacking Hate - [https://selma.swgfl.co.uk](https://selma.swgfl.co.uk/)

Scottish Anti-Bullying Service, Respectme - <http://www.respectme.org.uk/>

Scottish Government - Better relationships, better learning, better behaviour - <http://www.scotland.gov.uk/Publications/2013/03/7388>

DfE - Cyberbullying guidance - <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/374850/Cyberbullying_Advice_for_Headteachers_and_School_Staff_121114.pdf>

Childnet – Cyberbullying guidance and practical PSHE toolkit:

<http://www.childnet.com/our-projects/cyberbullying-guidance-and-practical-toolkit>

[Childnet – Project deSHAME – Online Sexual Harrassment](http://www.childnet.com/our-projects/project-deshame)

[UKSIC – Sexting Resources](https://www.saferinternet.org.uk/advice-centre/teachers-and-professionals/teaching-resources/sexting-resources)

Anti-Bullying Network – <http://www.antibullying.net/cyberbullying1.htm>

[Ditch the Label – Online Bullying Charity](https://www.ditchthelabel.org/)

[Diana Award – Anti-Bullying Campaign](http://www.antibullyingpro.com/)

### Social Networking

Digizen – [Social Networking](http://digizen.org/socialnetworking/)

UKSIC - [Safety Features on Social Networks](https://saferinternet.org.uk/guide-and-resource/social-media-guides)

[Children’s Commissioner, TES and Schillings – Young peoples’ rights on social media](https://www.tes.com/teaching-resources/digital-citizenship)

### Curriculum

53

SWGfL Evolve - [https://projectevolve.co.uk](https://projectevolve.co.uk/)

[UKCCIS – Education for a connected world framework](https://www.gov.uk/government/groups/uk-council-for-child-internet-safety-ukccis)

[Department for Education: Teaching Online Safety in Schools](https://www.gov.uk/government/publications/teaching-online-safety-in-schools)

Teach Today – [www.teachtoday.eu/](http://www.teachtoday.de/en/)

Insafe - [Education Resources](http://lreforschools.eun.org/web/guest/insafe)

### Data Protection

[360data - free questionnaire and data protection self review tool](http://360data.org.uk/)

[ICO Guides for Organisations](https://ico.org.uk/for-organisations/" \t "_blank)

[IRMS - Records Management Toolkit for Schools](https://irms.org.uk/general/custom.asp?page=SchoolsToolkit" \t "_blank)

[ICO Guidance on taking photos in schools](https://ico.org.uk/for-the-public/schools/photos/)

### Professional Standards/Staff Training

[DfE – Keeping Children Safe in Education](https://www.gov.uk/government/publications/keeping-children-safe-in-education--2)

DfE - [Safer Working Practice for Adults who Work with Children and Young People](https://www.gov.uk/government/publications/working-together-to-safeguard-children--2)

[Childnet – School Pack for Online Safety Awareness](http://www.childnet.com/resources/school-pack-for-online-safety-awareness)

[UK Safer Internet Centre Professionals Online Safety Helpline](http://www.saferinternet.org.uk/helpline)

### Infrastructure/Technical Support/Cyber-security

[UKSIC – Appropriate Filtering and Monitoring](https://www.saferinternet.org.uk/advice-centre/teachers-and-school-staff/appropriate-filtering-and-monitoring)

SWGfL Safety & [Security](https://swgfl.org.uk/resources/) Resources

Somerset - [Questions for Technical Support](https://www.somerset.org.uk/sites/edtech/eSafety/Leading/Questions%20for%20Technical%20Support%202018.pdf)

SWGfL - [Cyber Security in Schools](https://swgfl.org.uk/research/cyber-security-in-uk-schools/).

NCA – [Guide to the Computer Misuse Act](https://nationalcrimeagency.gov.uk/who-we-are/publications/75-guide-to-the-computer-misuse-act/file)

NEN –  [Advice and Guidance Notes](https://www.nen.gov.uk/advice/" \t "_blank)

### 

### Working with parents and carers

SWGfL – Online Safety Guidance [for](https://swgfl.org.uk/resources/online-safety-guidance-for-parents/) Parents & Carers

[Vodafone Digital Parents Magazine](http://www.vodafone.com/content/parents/digital-parenting.html)

[Childnet Webpages for Parents & Carers](http://www.childnet.com/parents-and-carers)

[Get Safe Online - resources for parents](https://www.getsafeonline.org/personal/article-category/safeguarding-children/" \t "_blank)

[Teach Today - resources for parents workshops/education](http://www.teachtoday.de/en/" \t "_blank)

[Internet Matters](https://www.internetmatters.org/)

### Prevent

[Prevent Duty Guidance](https://www.gov.uk/government/publications/prevent-duty-guidance)

[Prevent for schools – teaching resources](http://www.preventforschools.org/)

Childnet – [Trust Me](https://www.childnet.com/resources/trust-me)

### Research

[Ofcom –Media Literacy Research](https://www.ofcom.org.uk/research-and-data/media-literacy-research)

[Ofsted: Review of sexual abuse in schools and colleges](https://www.gov.uk/government/publications/review-of-sexual-abuse-in-schools-and-colleges/review-of-sexual-abuse-in-schools-and-colleges)

Further links can be found at the end of the UKCIS [Education for a Connected World Framework](https://www.gov.uk/government/publications/education-for-a-connected-world)

## C3 Glossary of Terms

**AUP/AUA** Acceptable Use Policy/Agreement – see templates earlier in this document

**CEOP** Child Exploitation and Online Protection Centre (part of National Crime Agency, UK Police, dedicated to protecting children from sexual abuse, providers of the Think U Know programmes.

**CPD** Continuous Professional Development

**FOSI** Family Online Safety Institute

**ICO** Information Commissioners Office

**ICT** Information and Communications Technology

**INSET** In Service Education and Training

**IP address** The label that identifies each computer to other computers using the IP (internet protocol)

**ISP** Internet Service Provider

**ISPA** Internet Service Providers’ Association

**IWF** Internet Watch Foundation

**LA** Local Authority

**LAN** Local Area Network

**MAT** Multi Academy Trust

**MIS** Management Information System

**NEN** National Education Network – works with the Regional Broadband Consortia (e.g. SWGfL) to provide the safe broadband provision to schools across Britain.

55

**Ofcom** Office of Communications (Independent communications sector regulator)

**SWGfL** South West Grid for Learning Trust – the Regional Broadband Consortium of SW Local Authorities – is the provider of broadband and other services for schools and other organisations in the SW

**TUK** Think U Know – educational online safety programmes for schools, young people and parents.

**UKSIC** UK Safer Internet Centre – EU funded centre. Main partners are SWGfL, Childnet and Internet Watch Foundation.

**UKCIS** UK Council for Internet Safety

**VLE** Virtual Learning Environment (a software system designed to support teaching and learning in an educational setting,

**WAP** Wireless Application Protocol

56

54

57

A more comprehensive glossary can be found at the end of the UKCIS [Education for a Connected World Framework](https://www.gov.uk/government/publications/education-for-a-connected-world)

Copyright of the SWGfL School Online Safety Policy Templates is held by SWGfL. Schools and other educational institutions are permitted free use of the templates. Any person or organisation wishing to use the document for other purposes should seek consent from SWGfL and acknowledge its use.

Every reasonable effort has been made to ensure that the information included in this template is accurate, as at the date of publication in January 2025. However, SWGfL cannot guarantee its accuracy, nor can it accept liability in respect of the use of the material whether in whole or in part and whether modified or not. Suitable legal/professional advice should be sought if any difficulty arises in respect of any aspect of this new legislation or generally to do with school conduct or discipline.

© SWGfL 2025

1. In a small school some of the roles described may be combined, though it is important to ensure that there is sufficient ‘separation of responsibility’ should this be the case. [↑](#footnote-ref-2)
2. See flow chart on dealing with online safety incidents in ‘[Responding to incidents of misuse’](#_Reporting_and_responding) and relevant local authority/MAT/ HR/other relevant body disciplinary procedures. [↑](#footnote-ref-3)