Grange Primary School

Online Safety Policy

Date of Last Review: June 2025
Policy Approved by Governing Body on: 6 June 2025
Next Review Date: June 2027

The original template and guidance for this policy was produced by South West Grid for Learning. It has been adapted to suit our school needs.

Links to our values as a Rights Respecting School:

As a Rights Respecting School, this policy relates to UNICEF rights under the Convention on the Rights of the Child:

Article 16: Protection of privacy: This article protects children's right to privacy, including their right to have their personal information kept confidential. In the online context, this means that children should be aware of the importance of protecting their personal information and should be careful about what they share online. They should also be aware of the privacy settings on social media platforms and other online services, and they should take steps to protect their privacy.

Article 17: Access to information: This article guarantees children's right to access information from a variety of sources. In the online context, this means that children should have access to a wide range of information and resources online. However, they should also be critical consumers of information and should be able to evaluate the credibility of online sources.

Article 19: Protection from abuse and neglect: This article protects children from all forms of abuse and neglect, including online abuse. In the online context, this means that children should be protected from cyberbullying, online grooming, and other forms of online abuse. They should also be aware of the dangers of sharing personal information with strangers online.

As duty bearers, at Grange Primary School, we understand the importance of upholding these rights to ensure the safety of all children.

1. Creating an Online Safety Ethos

1.1 Aims and policy scope

This Online Safety Policy outlines the commitment of Grange Primary School to safeguard members of our school community online in accordance with statutory guidance, including "Keeping Children Safe in Education (KCSIE)", and best practice.

This Online Safety Policy applies to all members of the school community (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).

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

Grange Primary School believes that online safety is an essential element of safeguarding children and adults in the digital world when using technology such as computers, tablets, mobile phones, or game consoles. This is a key tenet of Keeping Children Safe in Education (KCSIE).

Grange Primary School identifies that the internet and information communication technologies are an important part of everyday life, so children must be supported to be able to learn how to develop strategies to manage and respond to risk and be empowered to build resilience online.

Grange Primary School has a duty to provide the community with quality internet access to raise education standards, promote achievement, support the professional work of staff, and enhance management functions.

Grange Primary School identifies that there is a clear duty to ensure that all children and staff are protected from potential harm online.

The purpose of Grange Primary School's Online Safety Policy is to:

- Clearly identify the key principles expected of all members of the community with regards to the safe and responsible use of technology to ensure that Grange Primary School is a safe and secure environment.
- Safeguard and protect all members of the Grange Primary School community online, in line with KCSIE.
- Raise awareness with all members of the Grange Primary School community regarding the potential risks as well as the benefits of technology.
- Enable all staff to work safely and responsibly, to role model positive behaviour online, and be aware of the need to manage their own standards and practice when using technology.
- Identify clear procedures to use when responding to online safety concerns that are known by all members of the community.

This policy applies to all staff including the governing body, teachers, support staff, visitors, volunteers, and other individuals who work for or provide services on behalf of the school (collectively referred to as 'staff' in this policy) as well as children and parents/carers.

This policy applies to all access to the internet and use of information communication devices, including personal devices, or where children, staff, or other individuals have been provided with school-issued devices for use off-site, such as work laptops, tablets, or mobile phones.

This policy must be read in conjunction with other relevant school policies including (but not limited to) safeguarding and child protection (which reflects current KCSIE guidance), anti-bullying, behaviour, Acceptable Use Policies, GDPR Workforce & Pupil Privacy Notices, Staff Code of Conduct, and relevant curriculum policies.

1.2 Reviewing the online safety policy

- The Designated Safeguarding Lead (DSL) is Ms C Taylor (Headteacher).
- The Back-up DSL is Mr J Thackway (Deputy Headteacher).
- The Computing Subject Leader is Mrs B Mashiter.
- The Online Safety (e-Safety) lead for the Governing Body is Ms E Hick.

This Online Safety Policy was approved by the *school governing body on:*	*Insert date*
The implementation of this Online Safety Policy will be monitored by:	*Senior Leadership Team (including DSL)*
Monitoring will take place at regular intervals:	*Termly – Reported at Full Governors Meeting*
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 – Reported at Full Governors Meeting*
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:	*June 2026*
Should serious online safety incidents take place, the following external persons/agencies should be informed:	*Lancashire County Council* *Police*

1.3 Process for monitoring the impact of the Online Safety Policy

The school will monitor the impact of the policy using:

- Logs of reported incidents.
- Filtering and monitoring logs.
- Internal monitoring data for network activity.
- Surveys/questionnaires of:
  - learners
  - parents and carers
  - staff
- Governor updates.
- Leadership reviews.

1.3.1 The key responsibilities of the school management and leadership team are:

- Developing, owning, and promoting the online safety vision and culture to all stakeholders, in line with national and local recommendations, with appropriate support and consultation throughout the school community.
- Ensuring that online safety is viewed by the whole community as a safeguarding issue, as outlined in KCSIE, and proactively developing a robust online safety culture.
- Supporting the Designated Safeguarding Lead (DSL) by ensuring they have sufficient time and resources to fulfil their online safety role and responsibilities, including access to updated training every two years as recommended by KCSIE.
- Ensuring there are appropriate and up-to-date policies and procedures regarding online safety, including an Acceptable Use Policy which covers appropriate professional conduct and use of technology.
- To ensure that suitable and appropriate filtering and monitoring systems are in place to protect children from inappropriate content that meet the needs of the school community whilst ensuring children have access to required educational material, in line with DfE standards.
- To work with and support technical staff in monitoring the safety and security of school systems and networks and to ensure that the school network system is actively monitored.
- Ensuring all members of staff receive regular, up-to-date, and appropriate training regarding online safety roles and responsibilities (at least annually, in line with KCSIE recommendations) and providing guidance regarding safe and appropriate communications.
- Ensuring that online safety is embedded within a progressive whole-school curriculum which enables all pupils to develop an age-appropriate understanding of online safety and the associated risks and safe behaviours.
- To be aware of any online safety incidents and ensure that external agencies and support are liaised with as appropriate.
- Receiving and regularly reviewing online safeguarding records and using them to inform and shape future practice.
- Ensuring there are robust reporting channels for the school community to access regarding online safety concerns, including internal, local, and national support.
- To ensure a member of the Governing Body is identified with a lead responsibility for supporting online safety.

- Auditing and evaluating current online safety practice to identify strengths and areas for improvement.
- Ensure sufficient and appropriate separation of responsibilities.

1.3.2 The key responsibilities of the Designated Safeguarding Lead are:

- Acting as a named point of contact on all online safeguarding issues and liaising with other members of staff and other agencies as appropriate, as defined in KCSIE.
- Receiving relevant and regularly updated training in online safety, to the level recommended by KCSIE (typically every two years for DSLs and deputies), 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.
- Keeping up-to-date with current research, legislation (including KCSIE updates), and trends regarding online safety.
- Ensuring that online safety is promoted to parents and carers and the wider community through a variety of channels and approaches, including participation in local and national events to promote positive online behaviour, e.g., Safer Internet Day.
- Working with the school lead for data protection and data security to ensure that practice is in line with current legislation.
- Maintaining a record of online safety concerns/incidents and actions taken as part of the school's safeguarding recording structures and mechanisms using existing child protection/safeguarding procedures and templates.
- Monitoring the school's online safety incidents to identify gaps/trends and use this data to update the school's education response to reflect the need.
- To report to the school management team, Governing Body, and other agencies as appropriate, on online safety concerns and local data/figures.
- Liaising with the local authority and other local and national bodies, as appropriate.
- Working with the school leadership and management to review and update the online safety policies, Acceptable Use Policies (AUPs), and other related policies on a regular basis (at least annually) with stakeholder input.
- Ensuring that online safety is integrated with other appropriate school policies and procedures.
- Communicating regularly with the SLT & governor member with a lead responsibility for online safety.
- Liaising with staff and IT providers on matters of safety and safeguarding and welfare (including online and digital safety).

1.3.3 The key responsibilities for all members of staff are:

- Understanding that online safety is a core part of safeguarding, as emphasized in KCSIE.
- Contributing to the development of online safety policies.
- Reading the school Acceptable Use Policies (AUPs) and adhering to them.
- Taking responsibility for the security of school systems and data.
- Having an awareness of a range of different online safety matters/trends and how they may relate to the children in their care.
- Modelling good practice when using new and emerging technologies.
- Embedding online safety education in curriculum delivery wherever possible.
- Identifying individuals of concern and taking appropriate action by following school safeguarding policies and procedures, including KCSIE guidance.

- Knowing when and how to escalate online safety issues, internally and externally.
- Being able to signpost to appropriate support available for online safety issues, internally and externally.
- Understanding that all digital communications with learners and parents/carers are on a professional level and only carried out using official school systems.
- Maintaining a professional level of conduct in their personal use of technology, both on and off site, as outlined in the Staff Code of Conduct.
- Supervising and monitoring the use of digital technologies, mobile devices, cameras, etc., in lessons and other school activities (where allowed) and implementing current policies regarding these devices.
- 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 (including KCSIE) and local safeguarding policies (including the guidance contained in the SWGfL Safe Remote Learning Resource or current school equivalent), demonstrating an emphasis on positive learning opportunities.
- Taking personal responsibility for professional development in this area, including engaging with at least annual online safety updates.

1.3.4 In addition to the above, the key responsibilities for the Governing Body are:

- The Link Governor is to meet regularly with the Designated Safeguarding Lead / Online Safety Lead.
- Regularly receiving (collated and anonymised) reports of online safety incidents.
- Checking that provisions outlined in the Online Safety Policy (e.g., online safety education provision and staff training, including DSL training frequency) are taking place as intended and are compliant with KCSIE.
- 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.
- Reporting to relevant governors' meetings.
- Receiving (at least) basic cyber-security training to enable the governors to check that the school meets the DfE Cyber-Security Standards.

1.3.5 The key responsibilities for staff managing the technical environment are:

- Providing a safe and secure technical infrastructure which supports safe online practices while ensuring that learning opportunities are still maximised.
- Taking responsibility for the implementation of safe security of systems and data in partnership with the leadership and management team.
- To ensure that suitable access controls and encryption are implemented to protect personal and sensitive information held on school-owned devices.
- Ensuring that the school's filtering policy is applied and updated on a regular basis and that responsibility for its implementation is shared with the DSL.
- Ensuring that the use of the school's network is regularly monitored and reporting any deliberate or accidental misuse to the DSL.

- Reporting any breaches or concerns to the DSL and leadership team and together ensuring that they are recorded and appropriate action is taken as advised.
- Developing an understanding of the relevant legislation as it relates to the security and safety of the technical infrastructure.
- Reporting any breaches and liaising with the local authority (or other local or national bodies) as appropriate on technical infrastructure issues.
- Providing technical support and perspective to the DSL and leadership team, especially in the development and implementation of appropriate online safety policies and procedures.
- Ensuring that the school's ICT infrastructure/system is secure and not open to misuse or malicious attack.
- Ensuring that appropriate anti-virus software and system updates are installed and maintained on all school machines and portable devices.
- Ensuring that appropriately strong passwords are applied and enforced for all but the youngest users.
- The filtering policy is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person.

1.3.6 The key responsibilities of children and young people are:

- Contributing to the development of online safety policies.
- Reading the school's Acceptable Use Policies (AUPs) and adhering to them.
- Respecting the feelings and rights of others both on and offline.
- Seeking help from a trusted adult if things go wrong, and supporting others that may be experiencing online safety issues.
- At a level that is appropriate to their individual age, ability, and vulnerabilities:
  - Taking responsibility for keeping themselves and others safe online.
  - Taking responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.
  - Assessing the personal risks of using any particular technology and behaving safely and responsibly to limit those risks.

1.3.7 The key responsibilities of parents and carers are:

- Reading and signing the school's Acceptable Use Policies, encouraging their children to adhere to them, and adhering to them themselves where appropriate.
- Discussing online safety issues with their children, supporting the school in their online safety approaches, and reinforcing appropriate safe online behaviours at home.
- Role modelling safe and appropriate uses of technology and social media.
- Identifying changes in behaviour that could indicate that their child is at risk of harm online.
- Seeking help and support from the school, or other appropriate agencies, if they or their child encounters online problems or concerns.
- Using school systems, such as learning platforms, and other network resources, safely and appropriately.
- Taking responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.

1.3.8 The key responsibilities of Community Users are:

- Community users who access school systems/website/learning platform as part of the wider school provision will be expected to sign a community user AUP before being provided with access to school systems.

2. Managing Online Safety Concerns

2.1 Handling online safety concerns

All staff will be aware that technology is a significant component in many safeguarding and wellbeing issues affecting young people, particularly owing to the rise of social media and the increased prevalence of children using the internet. All procedures will be managed in line with KCSIE.

The DSL has overall responsibility for the school's approach to online safety and will ensure that there are strong processes in place to handle any concerns about pupils' safety online. The DSL should liaise with the police or children's social care services for support responding to harmful online sexual behaviour.

Any disclosures made by pupils to staff members about online abuse, harassment, or exploitation, whether they are the victim or disclosing on behalf of another child, will be handled in line with the Child Protection and Safeguarding Policy.

Staff will be aware that harmful online sexual behaviour can progress on a continuum, and appropriate and early intervention can prevent abusive behaviour in the future. Staff will also acknowledge that pupils displaying this type of behaviour are often victims of abuse themselves and should be suitably supported.

The victim of online harmful sexual behaviour may ask for no one to be told about the abuse. The DSL will consider whether sharing details of the abuse would put the victim in a more harmful position, or whether it is necessary in order to protect them from further harm, always acting in the child's best interests and in line with KCSIE. Ultimately, the DSL will balance the victim's wishes against their duty to protect the victim and other young people. The DSL and other appropriate staff members will meet with the victim's parents to discuss the safeguarding measures that are being put in place to support their child and how the report will progress.

Confidentiality will not be promised, and information may still be shared lawfully, for example, if the DSL decides that there is a legal basis under UK GDPR such as the public task basis whereby it is in the public interest to share the information. If the decision is made to report abuse to children's social care or the police against the victim's wishes, this must be handled extremely carefully - the reasons for sharing the information should be explained to the victim and appropriate specialised support should be offered.

Concerns regarding a staff member's online behaviour are reported to the headteacher, who decides on the best course of action in line with the relevant policies and KCSIE

guidance on allegations against staff. If the concern is about the headteacher, it is reported to the chair of governors.

Concerns regarding a pupil's online behaviour are reported to the DSL, who investigates concerns with relevant staff members, e.g., the headteacher and ICT technicians, and manages concerns in accordance with relevant policies depending on their nature, e.g., the Behaviour Policy and Child Protection and Safeguarding Policy.

Where there is a concern that illegal activity has taken place, the headteacher contacts the police.

The school avoids unnecessarily criminalising pupils, e.g., calling the police, where criminal behaviour is thought to be inadvertent and as a result of ignorance or normal developmental curiosity, e.g., a pupil has taken and distributed indecent imagery of themselves. The DSL will decide in which cases this response is appropriate and will manage such cases in line with the Child Protection and Safeguarding Policy.

All significant online safety incidents and the school's response are recorded by the DSL.

2.2 Cyberbullying

Cyberbullying can include, but is not limited to, the following:

- Threatening, intimidating, or upsetting text messages.
- Threatening or embarrassing pictures and video clips sent via mobile phone cameras.
- Silent or abusive phone calls or using the victim's phone to harass others, to make them think the victim is responsible.
- Threatening or bullying emails, possibly sent using a pseudonym or someone else's name.
- Unpleasant messages sent via instant messaging.
- Unpleasant or defamatory information posted to blogs, personal websites, and social networking sites, e.g., Facebook.
- Abuse between young people in intimate relationships online, i.e., teenage relationship abuse.
- Discriminatory bullying online, i.e., homophobia, racism, misogyny/misandry.

The school will be aware that certain pupils can be more at risk of abuse and/or bullying online, such as LGBTQ+ pupils and pupils with SEND, and will act in accordance with KCSIE to support them.

Cyberbullying against pupils or staff is not tolerated under any circumstances. Incidents of cyberbullying are dealt with quickly and effectively wherever they occur in line with the Anti-bullying Policy.

2.3 Child-on-child sexual abuse and harassment

Pupils may also use the internet and technology as a vehicle for sexual abuse and harassment. This is explicitly addressed within KCSIE. Staff will understand that this abuse can occur both in and outside of school, off and online, and will remain aware that pupils are less likely to report concerning online sexual behaviours, particularly if they are using websites that they know adults will consider to be inappropriate for their age.

The following are examples of online harmful sexual behaviour of which staff will be expected to be aware:

- Threatening, facilitating, or encouraging sexual violence.
- Upskirting, i.e., taking a picture underneath a person's clothing without consent and with the intention of viewing their genitals, breasts, or buttocks.
- Sexualised online bullying, e.g., sexual jokes or taunts.
- Unwanted and unsolicited sexual comments and messages.
- Consensual or non-consensual sharing of sexualised imagery.
- Abuse between young people in intimate relationships online, i.e., teenage relationship abuse.

All staff will be aware of and promote a zero-tolerance approach to sexually harassing or abusive behaviour, and any attempts to pass such behaviour off as trivial or harmless. Staff will be aware that allowing such behaviour could lead to a school culture that normalises abuse and leads to pupils becoming less likely to report such conduct.

Staff will be aware that creating, possessing, and distributing indecent imagery of other children, i.e., individuals under the age of 18, is a criminal offence, even where the imagery is created, possessed, and distributed with the permission of the child depicted, or by the child themselves.

The school will be aware that interactions between the victim of online harmful sexual behaviour and the alleged perpetrator(s) are likely to occur over social media following the initial report, as well as interactions with other pupils taking "sides", often leading to repeat harassment. The school will respond to these incidents in line with the Child-on-child Abuse Policy.

The school will respond to all concerns regarding online child-on-child sexual abuse and harassment, regardless of whether the incident took place on the school premises or using school-owned equipment. Concerns regarding online child-on-child abuse will be reported to the DSL, who will investigate the matter in line with the Child-on-child Abuse Policy and the Child Protection and Safeguarding Policy, following KCSIE procedures.

---

3. Online Communication and Safer Use of Technology

3.1 Managing the school website

- The school will ensure that information posted on the school website meets the requirements as identified by the Department for Education (DfE).
- The contact details on the website will be the school address, email, and telephone number. Staff or pupils' personal information will not be published without explicit, informed consent.
- The headteacher will take overall editorial responsibility for online content published and will ensure that information is accurate and appropriate.

- The website will comply with the school's guidelines for publications including accessibility, respect for intellectual property rights, privacy policies, and copyright.
- The administrator account for the school website will be safeguarded with an appropriately strong password.
- The school will post information about safeguarding, including online safety, on the school website for members of the community.
- Access to information and features will be tiered depending on school role.
- Each year a school governor and DSL/Online Safety Lead will take part in a website review with the website domain hosts.

3.2 Publishing images and videos online

- The school will ensure that all images and videos shared online are used in accordance with the school image use policy.
- The school will ensure that all use of images and videos takes place in accordance with other policies and procedures including data security, Acceptable Use Policies, Codes of Conduct, and the Use of Social Networking Sites and Other Forms of Social Media policy.
- Written permission from parents or carers will be obtained before images/videos of pupils are electronically published.
- Grange Primary School fully complies with GDPR (May 2018) and has issued privacy notices for the workforce and pupils. Consent is unbundled, and staff/pupils understand their rights under GDPR as detailed in the privacy notices. This means consent is specific, granular, and not tied to other services.

3.3 Managing email

- Pupils may only use school-provided email accounts for educational purposes.
- Members of staff will be provided with a specific school email address to use for any official communication.
- The forwarding of any chain messages/emails etc. is not permitted. Spam or junk mail will be blocked and reported to the email provider.
- Any electronic communication which contains any content which could be subject to data protection legislation (e.g., sensitive or personal information) will only be sent using secure and encrypted email.
- Access to school email systems will always take place in accordance with data protection legislation and in line with other appropriate school policies, e.g., confidentiality.
- Members of the community must immediately tell a designated member of staff if they receive offensive communication, and this will be recorded in the school safeguarding files/records.
- Staff will be encouraged to develop an appropriate work-life balance when responding to email.
- School email addresses and other official contact details will not be used for setting up personal social media accounts.

3.4 Official video-conferencing and webcam use for educational purposes

The school acknowledges that videoconferencing is a challenging activity with a wide range of learning benefits. Preparation and evaluation are essential to the whole activity.

- All videoconferencing equipment will be switched off when not in use and where appropriate, not set to auto-answer.
- Equipment connected to the educational broadband network will use the national E.164 numbering system and display their H.323 ID name. External IP addresses will not be made available to other sites.
- Videoconferencing contact details will not be posted publicly.
- Video conferencing equipment will be kept securely and, if necessary, locked.
- School videoconferencing equipment will not be taken off school premises without permission.
- Staff will ensure that external videoconference opportunities and/or tools are suitably risk-assessed and will ensure that accounts and systems used to access events are appropriately safe and secure.

Users:

- Videoconferencing settings are disabled for pupil devices.
- Parents' and carers' consent will be obtained prior to children taking part in videoconferencing activities.
- Video conferencing will take place via official and approved communication channels following a robust risk assessment.
- Only key administrators will be given access to videoconferencing administration areas or remote control pages.
- Unique log-on and password details for the educational videoconferencing services will only be issued to members of staff and kept secure.
- When recording a videoconference lesson, written permission will be given by all sites and participants. The reason for the recording must be given and the recording of videoconference should be clear to all parties at the start of the conference.
- Recorded material will be stored securely.
- If third-party materials are to be included, the school will check that recording is acceptable to avoid infringing the third party's intellectual property rights.
- The school will establish dialogue with other conference participants before taking part in a videoconference. If it is a non-school site, the school will check that they are delivering material that is appropriate for the class.

3.5 Appropriate and safe classroom use of the internet and any associated devices

Internet use is a key feature of educational access, and all children will receive age- and ability-appropriate education to support and enable them to develop strategies to respond to concerns as part of an embedded whole-school curriculum, as advocated by KCSIE. Please access specific curriculum policies for further information.

The school's internet access will be designed to enhance and extend education. Access levels to the internet will be reviewed to reflect the curriculum requirements and the age and ability of pupils.

All members of staff are aware that they cannot rely on filtering alone to safeguard children; supervision, classroom management, and education about safe and responsible use are essential components of safeguarding, as highlighted in KCSIE.

Supervision of pupils will be appropriate to their age and ability.

- At Early Years Foundation Stage and Key Stage 1, pupils' access to the internet will be by adult demonstration with occasional directly supervised access to specific and approved online materials which support the learning outcomes planned for the pupils' age and ability.
- At Key Stage 2, pupils will be supervised. Pupils will use age-appropriate search engines and online tools, and online activities will be teacher-directed where necessary. Children will be directed to online material and resources which support the learning outcomes planned for the pupils' age and ability.

All school-owned devices will be used in accordance with the school Acceptable Use Policy and with appropriate safety and security measures in place. Members of staff will always evaluate websites, tools, and apps fully before use in the classroom or recommending for use at home.

Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval, and evaluation. The school will ensure that the use of Internet-derived materials by staff and pupils complies with copyright law and acknowledges the source. Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

The evaluation of online materials is a part of teaching and learning in every subject and will be viewed as a whole-school requirement across the curriculum. The school will use the internet to enable pupils and staff to communicate and collaborate in a safe and secure environment.

Generative artificial intelligence (AI)

- The school will take steps to prepare pupils for changing and emerging technologies, e.g., generative AI, and how to use them safely and appropriately with consideration given to pupils' age.
- The school will ensure its IT system includes appropriate filtering and monitoring systems to limit pupils' ability to access or create harmful or inappropriate content through generative AI.
- The school will ensure that pupils are not accessing or creating harmful or inappropriate content, including through generative AI.
- The school will take steps to ensure that personal and sensitive data is not entered into generative AI tools and that it is not identifiable.
- The school will make use of any guidance and support that enables it to have a safe, secure, and reliable foundation in place before using more powerful technology such as generative AI.

Network security

- Technical security features, such as anti-virus software, will be kept up-to-date and managed by ICT technicians. Firewalls will be switched on at all times. ICT technicians will review the firewalls on a weekly basis to ensure they are running correctly and to carry out any required updates.
- Staff and pupils will be advised not to download unapproved software or open unfamiliar email attachments and will be expected to report all malware and virus attacks to ICT technicians.
- All members of staff will have their own unique usernames and private passwords to access the school's systems. Pupils will be provided with their own unique username and private passwords appropriate to their key stage. Staff members and pupils will be responsible for keeping their passwords private. Passwords will have a minimum and maximum length and require a mixture of letters, numbers, and symbols to ensure they are as secure as possible.
- Passwords will expire after 90 days, after which users will be required to change them.
- Users will inform ICT technicians if they forget their login details, who will arrange for the user to access the systems under different login details. Users will not be permitted to share their login details with others and will not be allowed to log in as another user at any time. If a user is found to be sharing their login details or otherwise mistreating the password system, the headteacher will be informed and will decide the necessary action to take.
- Users will be required to lock access to devices and systems when they are not in use.

Filtering and monitoring online activity

- The governing board will ensure the school's ICT network has appropriate filters and monitoring systems in place and that it is meeting the DfE's 'Filtering and monitoring standards for schools and colleges'. The governing board will ensure 'over-blocking' does not lead to unreasonable restrictions as to what pupils can be taught with regards to online teaching and safeguarding.
- The DSL will ensure that specific roles and responsibilities are identified and assigned to manage filtering and monitoring systems and to ensure they meet the school's safeguarding needs, as outlined in KCSIE.
- The headteacher and ICT technicians will undertake a risk assessment to determine what filtering and monitoring systems are required. The filtering and monitoring systems the school implements will be appropriate to pupils' ages, the number of pupils using the network, how often pupils access the network, and the proportionality of costs compared to the risks. ICT technicians will undertake monthly checks on the filtering and monitoring systems to ensure they are effective and appropriate.
- Requests regarding making changes to the filtering system will be directed to the headteacher. Prior to making any changes to the filtering system, ICT technicians and the DSL will conduct a risk assessment. Any changes made to the system will be recorded by ICT technicians. Reports of inappropriate websites or materials will be made to an ICT technician immediately, who will investigate the matter and make any necessary changes.
- Deliberate breaches of the filtering system will be reported to the DSL and ICT technicians, who will escalate the matter appropriately. If a pupil has deliberately breached the filtering system, they will be disciplined in line with the Behaviour Policy.

If a member of staff has deliberately breached the filtering system, they will be disciplined in line with the Disciplinary Policy and Procedure.

- If material that is believed to be illegal is accessed, inadvertently or deliberately, this material will be reported to the appropriate agency immediately, e.g., the Internet Watch Foundation (IWF), CEOP, and/or the police.
- The school's network and school-owned devices will be appropriately monitored. All users of the network and school-owned devices will be informed about how and why they are monitored. Concerns identified through monitoring will be reported to the DSL who will manage the situation in line with the Child Protection and Safeguarding Policy.

---

4. Social Media Policy

4.1 General social media use

Expectations regarding safe and responsible use of social media will apply to all members of Grange Primary School and exist in order to safeguard both the school and the wider community, on and offline. Examples of social media may include blogs, wikis, social networking sites, forums, bulletin boards, multiplayer online gaming, apps, video/photo sharing sites, chatrooms, instant messengers, and many others.

All members of the Grange Primary School community will be encouraged to engage in social media in a positive, safe, and responsible manner at all times. Information about safe and responsible use of social media will be communicated clearly and regularly to all members of the Grange Primary School community.

The school will control pupil and staff access to social media and social networking sites whilst on site and when using school-provided devices and systems. The use of social networking applications during school hours for personal use is outlined in the Social Networking policy (if separate) or Staff AUP/Code of Conduct.

Any concerns regarding the online conduct of any member of the Grange Primary School community on social media sites should be reported to the leadership team and will be managed in accordance with policies such as anti-bullying, allegations against staff (following KCSIE procedures), behaviour, and safeguarding/child protection.

Any breaches of school policy may result in criminal, disciplinary, or civil action being taken, and this will depend upon the age of those involved and the circumstances of the wrong committed. Action taken will be in accordance with relevant policies, such as social media, code of conduct, anti-bullying, allegations against staff, behaviour, and safeguarding/child protection.

4.2 Official use of social media

Grange Primary School official social media channels are:

- School website: www.grange.lancs.sch.uk
- Meta Business Suite including Instagram and Facebook

- Tapestry online learning journal

Official use of social media sites by the school will only take place with clear educational or community engagement objectives with specific intended outcomes, e.g., increasing parental engagement. Official use of social media sites as communication tools will be risk-assessed and formally approved by the headteacher.

Official school social media channels will be set up as distinct and dedicated social media sites or accounts for educational or engagement purposes. Staff will use school-provided email addresses to register for and manage any official approved social media channels.

Members of staff running official social media channels will sign a specific Acceptable Use Policy (AUP) to ensure they are aware of the required behaviours and expectations of use and to ensure that sites are used safely, responsibly, and in accordance with local and national guidance and legislation.

All communication on official social media platforms will be clear, transparent, and open to scrutiny. Any online publication on official social media sites will comply with legal requirements including the Data Protection Act 2018 (incorporating GDPR), the right to privacy conferred by the Human Rights Act 1998, or similar duty to protect private information, and will not breach any common law duty of confidentiality, copyright, etc.

Official social media use will be in line with existing policies including anti-bullying and child protection. Images or videos of children will only be shared on official social media sites/channels in accordance with the image use policy and with unbundled parental consent.

Information about safe and responsible use of social media channels will be communicated clearly and regularly to all members of the community. Official social media sites, blogs, or wikis will be suitably protected (e.g., password-protected) and where possible/appropriate, run and/or linked to from the school website and take place with written approval from the Leadership Team.

Leadership staff must be aware of account information and relevant details for social media channels in case of emergency, such as staff absence. Parents/Carers and pupils will be informed of any official social media use, along with expectations for safe use and action taken to safeguard the community.

Public communications on behalf of the school will, where possible, be read and agreed by at least one other colleague. Official social media channels will link back to the school website and/or Acceptable Use Policy to demonstrate that the account is official. The school will ensure that any official social media use does not exclude members of the community who are unable or unwilling to use social media channels.

4.3 Staff personal use of social media

The safe and responsible use of social networking, social media, and personal publishing sites will be discussed with all members of staff as part of staff induction and will be revisited and communicated via regular staff training opportunities (at least annually).

Safe and professional behaviour will be outlined for all members of staff (including volunteers) as part of the school's policies including but not limited to the social networking policy (if separate), Staff Code of Conduct, and Acceptable Use Policy.

All members of staff are advised not to communicate with or add as 'friends' any current or past children/pupils or current or past pupils' family members via any personal social media sites, applications, or profiles. Any pre-existing relationships or exceptions that may compromise this will be discussed with the Designated Safeguarding Lead and/or the headteacher.

If ongoing contact with pupils is required once they have left the school roll, then members of staff will be expected to use existing alumni networks or use official school-provided communication tools.

All communication between staff and members of the school community on school business will take place via official approved communication channels (such as an official school-provided email address or phone numbers). Staff will not use personal social media accounts to make contact with pupils or parents, nor should any contact be accepted, except in circumstances whereby prior approval has been given by the Headteacher. Any communication from pupils/parents received on personal social media accounts will be reported to the school's designated safeguarding lead.

Information and content that staff members have access to as part of their employment, including photos and personal information about pupils and their family members, colleagues, etc., will not be shared or discussed on personal social media sites.

All members of staff are strongly advised to safeguard themselves and their privacy when using social media sites. This will include being aware of location-sharing services, setting the privacy levels of their personal sites as strictly as they can, opting out of public listings on social networking sites, logging out of accounts after use, and keeping passwords safe and confidential.

All members of staff are encouraged to carefully consider the information, including text and images, they share and post online and to ensure that their social media use is compatible with their professional role and is in accordance with school policies (safeguarding, confidentiality, data protection, etc.) and the wider professional and legal framework, including guidance in KCSIE regarding maintaining professional boundaries.

Members of staff will be encouraged to manage and control the content they share and post online. Advice will be provided to staff via staff training and by sharing appropriate guidance and resources on a regular basis.

Members of staff will notify the Leadership/Management Team immediately if they consider that any content shared or posted via any information and communications technology, including emails or social networking sites, conflicts with their role in the school.

Members of staff are encouraged not to identify themselves as employees of Grange Primary School on their personal social networking accounts. This helps prevent information

on these sites from being linked with the school and also safeguards the privacy of staff members and the wider community.

Members of staff will ensure that they do not represent their personal views as that of the school on social media. School email addresses will not be used for setting up personal social media accounts. Members of staff who follow/like the school social media channels will be advised to use dedicated professional accounts, where possible, to avoid blurring professional boundaries.

4.4 Staff official use of social media

- If members of staff are participating in online activity as part of their capacity as an employee of the school, then they are requested to be professional at all times and to be aware that they are an ambassador for the school.
- Staff using social media officially will disclose their official role/position but always make it clear that they do not necessarily speak on behalf of the school.
- Staff using social media officially will be responsible, credible, fair, and honest at all times and consider how the information being published could be perceived or shared.
- Staff using social media officially will always act within the legal frameworks they would adhere to within the workplace, including libel, defamation, confidentiality, copyright, data protection, as well as equalities laws.
- Staff must ensure that any image posted on any official social media channel has appropriate written parental consent, which is **unbundled** and specific.
- Staff using social media officially will be accountable and must not disclose information, make commitments, or engage in activities on behalf of the school unless they are authorised to do so.
- Staff using social media officially will inform the Designated Safeguarding Lead and/or the head teacher of any concerns such as criticism or inappropriate content posted online.
- Staff will not engage with any direct or private messaging with children or parents/carers through social media and will communicate via official communication channels.
- Staff using social media officially will comply with the school social networking policy (if separate) and Acceptable Use Policy.

4.5 Pupils' use of social media

- Safe and responsible use of social media sites will be outlined for children and their parents as part of the Acceptable Use Policy.
- Personal publishing on social media sites will be taught to pupils as part of an embedded and progressive education approach via age-appropriate sites which have been risk-assessed and approved as suitable for educational purposes.
- Pupils will be advised to consider the risks of sharing personal details of any kind on social media sites which may identify them and/or their location. Examples would include real/full name, address, mobile or landline phone numbers, school attended, Instant Messenger contact details, email addresses, full names of friends/family, specific interests, and clubs, etc.
- Pupils will be advised not to meet any online friends without a parent/carer or other responsible adult's permission and only when they can be present.

- Pupils will be advised on appropriate security on social media sites and will be encouraged to use safe passwords, deny access to unknown individuals, and be supported in learning how to block and report unwanted communications.
- Parents will be informed of any official social media use with pupils and written parental consent will be obtained, as required.
- Any official social media activity involving pupils will be moderated by the school where possible.
- The school is aware that many popular social media sites state that they are not for children under the age of 13; therefore, the School will not create accounts within school specifically for children under this age.
- Any concerns regarding pupils' use of social networking, social media, and personal publishing sites, both at home and at school, will be dealt with in accordance with existing school policies including anti-bullying and behaviour.
- Any concerns regarding pupils' use of social networking, social media, and personal publishing sites, both at home and at school, will be raised with parents/carers, particularly when concerning any underage use of social media sites.

---

5. Use of Personal Devices and Mobile Phones

5.1 Rationale regarding personal devices and mobile phones

The widespread ownership of mobile phones and a range of other personal devices among children, young people, and adults will require all members of the Grange Primary School community to take steps to ensure that mobile phones and personal devices are used responsibly.

The use of mobile phones and other personal devices by young people and adults will be decided by the school and is covered in appropriate policies including, but not limited to, the school Acceptable Use and safeguarding policies.

Grange Primary School recognises that personal communication through mobile technologies is an accepted part of everyday life for children, staff, and parents/carers but requires that such technologies need to be used safely and appropriately within schools.

5.2 Expectations for safe use of personal devices and mobile phones

- All use of personal devices and mobile phones will take place in accordance with the law and other appropriate school policies.
- Electronic devices of all kinds that are brought on site are the responsibility of the user at all times. The school accepts no responsibility for the loss, theft, or damage of such items. Nor will the school accept responsibility for any adverse health effects caused by any such devices, either potential or actual.
- Mobile phones and personal devices are not permitted to be used in certain areas within the school site such as changing rooms, toilets, and swimming pools.

- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the community, and any breaches will be dealt with as part of the discipline/behaviour policy.
- Members of staff will be issued with a work phone number and email address where contact with pupils or parents/carers is required.
- All members of the Grange Primary School community will be advised to take steps to protect their mobile phones or devices from loss, theft, or damage.
- All members of the Grange Primary School community will be advised to use passwords/pin numbers to ensure that unauthorised calls or actions cannot be made on their phones or devices if they are lost or stolen. Passwords and pin numbers should be kept confidential. Mobile phones and personal devices should not be shared.
- All members of the Grange Primary School community will be advised to ensure that their mobile phones and personal devices do not contain any content which may be considered to be offensive, derogatory, or would otherwise contravene the school's policies.
- School mobile phones and devices must always be used in accordance with the Acceptable Use Policy and any other relevant policies.
- School mobile phones and devices used for communication with parents and pupils must be suitably protected via a passcode/password/pin and must only be accessed and used by authorised members of staff.

5.3 Pupils' use of personal devices and mobile phones

- Pupils will be educated regarding the safe and appropriate use of personal devices and mobile phones.
- Pupils will be discouraged from bringing personal devices and mobile phones to school. If pupils do bring these devices, they will be expected to comply with acceptable user policies. The school will not accept liability for these devices (as outlined in section 5.2).
- Pupils will leave their personal devices in a central, secure location as directed by the school.
- If members of staff have an educational reason to allow children to use their mobile phones or personal devices as part of an educational activity, then it will only take place when approved by the Leadership Team.
- If a pupil needs to contact his/her parents/carers, they will be allowed to use a school phone.
- Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office. Exceptions may be permitted in exceptional circumstances on a case-by-case basis and as approved by the headteacher.
- If a pupil breaches the school policy, then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to parents/carers in accordance with the school policy.
- If there is suspicion that material on a pupil's personal device or mobile phone may be illegal or may provide evidence relating to a criminal offence, then the device will be handed over to the police for further investigation, following KCSIE guidance.

5.4 Staff use of personal devices and mobile phones

- Members of staff are not permitted to use their own personal phones or devices for contacting children, young people, and their families within or outside of the school in a professional capacity. Any pre-existing relationships which could compromise this will be discussed with leaders/managers.
- Staff will not use personal devices such as mobile, tablets or cameras to take photos or videos of children and will only use work-provided equipment for this purpose.
- Staff will not use any personal devices directly with children and will only use work-provided equipment during lessons/educational activities.
- Members of staff will ensure that any use of personal phones and devices will always take place in accordance with the law e.g. GDPR as well as relevant school policy and procedures including but not limited to social networking policy (if separate), Staff Code of Conduct, confidentiality, data security, Acceptable Use etc.
- Staff personal mobile phones and devices will be switched off/switched to 'silent' mode during lesson times.
- Bluetooth or other forms of communication should be "hidden" or switched off during lesson times.
- Personal mobile phones or devices will not be used during teaching periods unless permission has been given by a member of the Leadership Team in emergency circumstances.
- Staff will ensure that any content bought on site via mobile phones and personal devices are compatible with their professional role and expectations.
- If a member of staff breaches the school policy then disciplinary action will be taken.
- If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal device or have committed a criminal offence then the police will be contacted.
- Any allegations against members of staff involving personal use of mobile phone or devices will be responded to following the school's allegations management policy and KCSIE procedures.
- Staff/volunteers must be aware of those learners whose images must not be taken/published due to lack of consent or other safeguarding reasons. Those images should only be taken on school devices. The personal devices of staff should not be used for such purposes.

5.5 Visitors use of personal devices and mobile phones

- Parents/carers and visitors must use mobile phones and personal devices in accordance with the school acceptable use policy.
- Use of mobile phones or personal devices by visitors and parents/carers to take photos or videos must take place in accordance with the school image use policy.
- The school will ensure appropriate signage and information is displayed and provided to inform visitors of expectations of use.
- Staff will be expected to challenge concerns when safe and appropriate and will always inform the Designated Safeguarding Lead of any breaches of use by visitors.