High Wycombe
Church of England School

POLICY	**ONLINE SAFETY POLICY**
COMMITTEE:	PERSONNEL
MEMBER OF STAFF RESPONSIBLE:	SAM BIDDLE
GOVERNOR RESPONSIBLE:	CHAIR OF PERSONNEL
WRITTEN BY DATE:	2023
LAST UPDATED BY AND DATE:	CELINE HAWKINS SEPTEMBER 2023
REVIEWED BY AND DATE:	TABITHA CAROE JUNE 2025
REVIEW DATE:	JUNE 2026

Adopted from The Key Model Policy 2020

Contents

1. Policy Aims, Legislation & Guidance	3
2. Scope of the Policy	3
3. Roles & Responsibilities	4
4. Education & Engagement Approaches	9
5. Technical – infrastructure/equipment, filtering and monitoring – Safer Use of Technology	12
6. Links with other Policies	21
Appendix 1: Online Safety Contacts and Resources	22
Appendix 2: Parent / Carer Acceptable Use Agreement	23
Appendix 2a: EYFS and KS1 acceptable use agreement (pupils and parents/carers)	25
Appendix 2b: KS2 acceptable use agreement (pupils and parents/carers)	26
Appendix 2c: acceptable use agreement (staff, governors, volunteers and visitors)	27
Appendix 3: Social Media Policy	28
Appendix 4: Online Safety Training Needs: Self Audit for Staff	34

HIGH WYCOMBE CHURCH OF ENGLAND SCHOOL
ONLINE SAFETY POLICY
'BE STRONG AND COURAGEOUS'

1. Policy Aims, Legislation & Guidance

This policy takes into account the DfE statutory guidance "Keeping Children Safe in Education" and the following DfE advice:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation

It also refers to the Department's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum Computing programmes of study.

The purpose of this policy is to:

- Have robust processes in place in order to safeguard and protect all members of our community – pupils and their families, staff, volunteers and governors.
- Identify and deliver effective approaches to empower us to protect, educate and raise awareness of online safety throughout that community.
- Enable all staff to work safely and responsibly, to role model positive behaviour online and to manage professional standards and practice when using technology.
- Identify clear procedures to use when responding to online safety concerns.
- High Wycombe Church of England Combined School identifies that the issues classified within online safety are considerable, but can be broadly categorised into three areas of risk:
    1. Content: being exposed to illegal, inappropriate or harmful material
    2. Contact: being subjected to harmful online interaction with other users
    3. Conduct: personal online behaviour that increases the likelihood of, or causes, harm.

2. Scope of the Policy

This policy applies to all members of the school community (including governing body, staff, students, volunteers, parents/carers, visitors, community users, external contractors – collectively

referred to as 'staff' in this policy) who have access to and are users of school ICT systems, both in and out of the school.

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

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the school / academy site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other online safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

The school 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.

3. Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within the school:

3.1 Governors:

Governors are responsible for the approval and monitoring of the Online Safety Policy and for reviewing the effectiveness of the policy.

All governors will:

- Ensure they have read and understood this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet
- Attend regular meetings with the DSL and Computing Lead responsible for internet safety
- Regularly monitor any logged incidences concerning internet safety as part of school safeguarding processes
- Report to the relevant Governors/Board/Committee meeting.

3.2 Headteacher and Senior Leaders:

- The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the Computing subject leader.
- The Headteacher and members 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.

- The Headteacher and members of the Senior Leadership Team should ensure that online safety is viewed as a safeguarding issue and that practice is in line with national and local recommendations and requirements.
- The Headteacher is responsible for ensuring that the Computing subject leader and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The Headteacher should ensure there are appropriate and up-to-date policies regarding online safety; including a 'Code of Conduct' and/or an 'Acceptable Use Policy' (AUP) which covers acceptable use of technology
- The Headteacher 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. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Headteacher and Senior Leadership Team will work with technical staff to monitor the safety and security of school systems and networks.
- The Senior Leadership Team should ensure that online safety is embedded within a progressive whole school curriculum, which enables all pupils to develop an age-appropriate understanding of online safety.
- The Headteacher and Senior Leadership Team should ensure there are robust reporting channels for the school community to access regarding online safety concerns, including internal, local and national support.
- The Headteacher and Senior Leadership Team should ensure that appropriate risk assessments are undertaken regarding the safe use of technology. Audit and evaluate online safety practice to identify strengths and areas for improvement.

3.3 Computing Subject Leader:

- Takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies/ documents.
- Ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- Provides training and advice for staff.
- Liaises with school technical staff.
- Reports when necessary to Senior Leadership Team.
- Should work with staff to coordinate participation in local and national events to promote positive online behaviour, such as Safer Internet Day.
- Should ensure all members of staff receive regular, up to date and appropriate online safety training.
- Ensure that online safety is promoted to parents, carers and the wider community, through a variety of channels and approaches.
- Should maintain records (a log of incidents to inform future online safety developments) of online safety concerns, as well as actions taken, as part of the schools safeguarding recording mechanisms and report online safety concerns, as appropriate, to staff and Governing Body.
- Should be trained in up to date online safety issues in line with current research, legislation and trends and be aware of the potential for serious child protection / safeguarding issues to arise from:

- sharing of personal data;
- access to illegal / inappropriate materials;
- inappropriate on-line contact with adults / strangers;
- potential or actual incidents of grooming;
- cyber-bullying.

3.4 The Network Technical Staff (Turn It On):

Are responsible for ensuring:

- That the school's technical infrastructure is secure and is not open to misuse or malicious attack by putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material.
- That the school meets required online safety technical requirements and any Local Authority/other relevant body Online safety Policy/Guidance that may apply. That users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed.
- That 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.
- That the use of the network/internet/Virtual Learning Environment/website/remote-access/email/on-line learning is regularly monitored in order that any misuse/attempted misuse can be reported to the Headteacher for investigation.
- That monitoring software/systems are implemented and updated as agreed in school policies.

3.5 Teaching and Support Staff:

Are responsible for ensuring that:

- They have an up to date awareness of online safety matters and of the current school online safety policy and practices and can contribute to online safety policies
- They have read, understood and signed the Staff Acceptable Use Policy/Agreement (AUP)
- They model good practice when using technology and maintain a professional level of conduct in their personal use of technology both on and off site
- They report any suspected misuse or problem to the Headteacher/DSL for investigation by following the school's safeguarding policies and procedures and that incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy.
- They complete required online safety training and as a result have an awareness of online safety issues and how they may be experienced by the children in their care.
- All digital communications with students, parents/carers should be on a professional level and only carried out using official school systems for which they take responsibility – including responsibility for the data used.
- Online safety issues are embedded in all aspects of the curriculum and other activities.
- Students understand and follow the online safety and acceptable use policies.
- Students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.

- They monitor the use of digital technologies, mobile devices, tablets, cameras etc in lessons and other school activities and implement current policies with regard to these devices.
- In lessons where internet use is pre-planned students 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.
- Take personal responsibility for professional development in this area including all online training.

3.6 Designated Safeguarding Lead (DSL):

- Should act as a named point of contact on all online safeguarding issues and liaise with other members of staff or other agencies as appropriate
- Should work with staff to coordinate participation in local and national events to promote positive online behaviour, such as Safer Internet Day.
- Should ensure all members of staff receive regular, up to date and appropriate online safety training.
- Ensure that online safety is promoted to parents, carers and the wider community, through a variety of channels and approaches.
- Should maintain records of online safety concerns, as well as actions taken, as part of the schools safeguarding recording mechanisms and report online safety concerns, as appropriate, to staff and Governing Body.
- Should be trained in up to date online safety issues in line with current research, legislation and trends and be aware of the potential for serious child protection / safeguarding issues to arise from:
    - sharing of personal data;
    - access to illegal / inappropriate materials;
    - inappropriate on-line contact with adults / strangers;
    - potential or actual incidents of grooming;
    - cyber-bullying.

Further details of the school's DSL are set out in the Child Protection and Safeguarding Policy as well as relevant job descriptions.

3.7 Students (at a level that is appropriate to their individual age, ability and vulnerabilities):

- Are responsible for using the school digital technology systems in accordance with the Student Acceptable Use Policy and are responsible for their learning of how to use online resources correctly.
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking/use of images and on cyber-bullying.

- Should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online safety Policy covers their actions out of school, if related to their membership of the school.
- Should engage in age appropriate online safety education opportunities.
- Must respect the feelings and rights of others both on and offline.
- Should take responsibility for keeping themselves and others safe online.
- Should seek help from a trusted adult, if there is a concern online, and support others that may be experiencing online safety issues.

3.8 Parents / Carers:

Parents/Carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way by discussing online safety issues with their children. They should reinforce appropriate, safe online behaviours at home – including role-modelling safe and appropriate use of technology and social media themselves. Parents should try to identify changes in behaviour that could indicate that their child is at risk of harm online and seek help and support from the school or other appropriate agencies, if they or their child encounter risk or concerns online. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website/VLE and information about national/local online safety campaigns/literature.

Parents should abide by any home-school agreement and internet safety agreement.

Parents should take responsibility for their own awareness in relation to the risks and opportunities posed by new and emerging technologies. They should be responsible for understanding how the school's online resources function and undertake relevant training/instruction as appropriate.

Parents and carers will be encouraged to notify the school of any concerns regarding this policy and support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events;
- access to parents' sections of the website and on-line student/pupil records;
- their children's personal devices in the school/academy (where this is allowed).

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- Think U Know – https://www.thinkuknow.co.uk/ (accessible via the school's website)
- CEOP (Child Exploitation and Online Protection Command) – https://www.ceop.police.uk/Safety-Centre/ (accessible via the school's website)
- NSPCC – https://www.nspcc.org.uk/keeping-children-safe/onlinonline safety/ (accessible via the school's website)
- UK Safer Internet Centre - https://saferinternet.org.uk/guide-and-resource/what-are-the-issues
- Get Safe Online – getsafeonline.org
- Childnet – https://www.childnet.com/help-and-advice/parents-and-carers

- Childnet Parents and Carers Resource Sheet – https://www.childnet.com/resources/parents-and-carers-resource-sheet/

4. Education and Engagement Approaches

4.1 Education – students

Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students in online safety is therefore an essential part of the school's e- safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

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:

- The school teaches specific online safety lessons to children in KS1 and 2 that follow the Common Sense Education scheme. These lessons occur termly in KS1 and half-termly in KS2.
- Key online safety messages should be reinforced as part of a planned programme of assemblies and pastoral activities.
- Students should be taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information.
- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Students should be helped to understand the need for the student Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school.
- 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 students 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 students are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove 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 school will support pupils to understand their responsibilities by:
    - displaying acceptable use posters within the school;
    - informing pupils that network and internet use will be monitored for safety and security purposes and in accordance with legislation;
    - rewarding positive use of technology by pupils;

- providing online safety education and training as part of the transition programme across the key stages and when moving between establishments;
- using support, such as external visitors, where appropriate, to complement and support the school's internal online safety education approaches;
- use assemblies to raise pupils' awareness of the dangers that can be encountered online.

From September 2020 all schools will have to teach Relationships education and health education, which includes elements on online safety. This statutory guidance states that by the end of primary school, all pupils should know:

Relationships education:

- *that people sometimes behave differently online, including by pretending to be someone they are not;*
- *that the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous;*
- *the rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them;*
- *how to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met;*
- *how information and data is shared and used online;*
- *how to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know.*

Physical health and mental wellbeing:

- *that for most people the internet is an integral part of life and has many benefits;*
- *about the benefits of rationing time spent online, the risks of excessive time spent on electronic devices and the impact of positive and negative content online on their own and others' mental and physical wellbeing;*
- *how to consider the effect of their online actions on others and know how to recognise and display respectful behaviour online and the importance of keeping personal information private;*
- *why social media, some computer games and online gaming, for example, are age restricted;*
- *that the internet can also be a negative place where online abuse, trolling, bullying and harassment can take place, which can have a negative impact on mental health;*
- *how to be a discerning consumer of information online including understanding that information, including that from search engines, is ranked, selected and targeted;*
- *where and how to report concerns and get support with issues online.*

What this looks like in school:

In **Key Stage 1**, pupils will be taught to:

- use technology safely and respectfully, keeping personal information private;

- identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies.

Pupils in **Key Stage 2** will be taught to:

- use technology safely, respectfully and responsibly;
- recognise acceptable and unacceptable behaviour;
- identify a range of ways to report concerns about content and contact.

4.2 Education - Vulnerable Pupils

We are aware that some pupils are considered to be more vulnerable online due to a range of factors. This may include, but is not limited to, children in care, children with Special Educational Needs and Disabilities (SEND) or mental health needs, children with English as an additional language (EAL) and children experiencing trauma or loss.

We will:

- ensure that differentiated and ability appropriate online safety education, access and support is provided to vulnerable pupils;
- seek input from specialist staff as appropriate, including the SENDCo and DSL.

4.3 Education – parents / carers

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring/regulation of the children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

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

- Curriculum activities
- Letters, newsletters, web site
- High profile events/campaigns e.g. Safer Internet Day
- Reference to the relevant web sites / publications e.g. www.swgfl.org.uk, www.saferinternet.org.uk and www.childnet.com/parents-and-carers.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the headteacher.

4.4 Education & Training – Staff/Volunteers

It is essential that all staff 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 training will be made available to staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school Online safety Policy and Acceptable Use Agreements. Staff will be made aware that school systems are monitored and activity can be traced to individual users; staff will be reminded to behave professionally and in accordance with school's policies when accessing school systems and devices.
- Staff will be made aware that their online conduct out of school, including personal use of social media, could have an impact on their professional role and reputation within school. They will be reminded of their responsibilities on social media and WhatsApp groups etc. outside of school by referring them to the school's Social Media Policy.
- The Computing lead will receive regular updates through attendance at external training events.
- The Online safety Policy and its updates will be presented to and discussed by staff in staff meetings and INSET day to ensure all members of staff are aware of the procedures to follow regarding online safety concerns affecting pupils, colleagues or other members of the school community.
- The Computing lead will provide advice/guidance/training to individuals as required.
- Useful educational resources and tools that staff should use, according to the age and ability of the pupils will be highlighted for potential use.
- The DSL will undertake child protection and safeguarding training, which will include online safety, at least every two years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

5. Technical – infrastructure/equipment, filtering and monitoring – Safer Use of Technology

The internet is an essential element for education, business and social interaction. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils, and so the school has a duty to provide the pupils with quality internet access as part of their learning experience:

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements.
- There will be regular reviews and audits of the safety and security of school technical systems.
- Servers, wireless systems and cabling must be securely located and physical access restricted.
- All users will have clearly defined access rights to school technical systems and devices.
- All year groups have class group logons that all members can access.
- The "master/administrator" passwords for the school ICT system, used by the Network Manager must also be available to the Headteacher and kept in a secure place.
- Internet access is filtered for all users. Illegal content is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list.

- Users to report any actual/potential technical incident/security breach to Turn It On/ CPOMS /Site Manager / GDPR lead.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work-stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. The school infrastructure and individual workstations are protected by up to date virus software.
- An Acceptable Use Agreement is in place for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the school systems.
- An agreement is signed by each member of staff regarding the extent of personal use that users (staff/ students/ pupils/ community users) and their family members are allowed on school devices that may be used out of school.

5.1 Own devices in school

The educational opportunities offered by mobile technologies are being expanded as a wide range of devices, software and online services become available for teaching and learning, within and beyond the classroom. This has led an increasing number of staff bringing their own devices to school in order to provide a greater freedom of choice and usability. However, there are a number of online safety considerations that need to be reviewed as a result of this.

- The school has a set of clear expectations and responsibilities for all users.
- The school adheres to the Data Protection Act principles.
- All users are provided with and accept the Acceptable Use Agreement.
- Where possible these devices will be covered by the school's normal filtering systems, while being used on the premises.
- All users will use their username and password and keep this safe.

5.2 Staff using work devices outside school

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use. Work devices must be used solely for work activities.

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. Any USB devices containing data relating to the school must be encrypted.

If staff have any concerns over the security of their device, they must seek advice from Turn It On.

5.3 Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and students need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for

cyberbullying 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.

- When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other students 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, distribution and publication of those images. Those images should only be taken on school equipment; personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital/video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Students must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images.
- Students' full names will not be used anywhere on a website or social media, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of students are published on the school website (covered as part of the GDPR consent form signed by parents or carers at the start of the year).

5.4 Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- fairly and lawfully processed;
- processed for limited purposes;
- adequate, relevant and not excessive;
- accurate;
- kept no longer than is necessary;
- processed in accordance with the data subject's rights;
- secure;

- only transferred to others with adequate protection.

The school must ensure that:

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing".

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.
- 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 and secure password protected devices. When personal data is stored on any portable computer system, memory stick or any other removable media:
    - the data must be encrypted and password protected;
    - the device must be password protected (many memory sticks/ cards and other mobile devices cannot be password protected);
    - the device must offer approved virus and malware checking software;
    - the data must be securely deleted from the device, in line with school policy once it has been transferred or its use is complete.

For further details, see the school's Data Protection (GDPR) Policy and how it links to internet safety.

5.5 Communications

Rapidly developing communications technologies have the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs the risks/disadvantages:

	Staff & other adults				**Pupils**			
Communication technologies	Not allowed	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission

Mobile phones may be brought to school*		✓			✓			
Use of mobile phones in lessons	✓				✓			
Use of mobile phones in social time		✓						
Taking photos on mobile phones/cameras			✓					
Use of other mobile devices e.g., tablets, gaming devices			✓					
Use of personal email addresses in school, or on school network			✓					
Use of messaging apps			✓					
Use of social media			✓					
Use of blogs			✓					

* Year 6 pupils have permission to bring named mobile phones to school on the condition that this is done so with parental consent and that their device is left in the school office at the beginning of the school day and collected just before being dismissed from school.

5.6 Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- cause harm, and/or
- disrupt teaching, and/or
- break any of the school rules.

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- delete that material, or
- retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- report it to the police.

Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation.
Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

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

- The official school email service is regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and students should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access).

- Users must immediately report, to the DSL, 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.
- Any digital communication between staff and students or parents/carers (email, chat, VLE etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Students should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

5.7 Social Media - Protecting Professional Identity

With an increase in use of all types of social media for professional and personal purposes a policy that sets out clear guidance for staff to manage risk and behaviour online is essential. Core messages should include the protection of pupils, the school and the individual when publishing any material online. Expectations for teachers' professional conduct are set out in 'Teachers Standards 2012', while DfE's online safety framework 2023 reviews how a school protects and educates staff and pupils in their use of technology, including what measures would be expected to be in place to intervene and support should a particular issue arise.

All schools, academies and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school or local authority liable to the injured party.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through limiting access to personal information:

- Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions.
- Risk assessment, including legal risk.

School staff should ensure that:

- no reference should be made in social media to students/pupils, 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 or local authority;
- security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information;
- the school's use of social media for professional purposes will be checked regularly by the GDPR lead to ensure compliance with the Social Media (see Appendix 3) and Data Protection (GDPR) policies.

5.8 Unsuitable / inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other technical systems. Other activities e.g. cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities.

Users shall not visit internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:

- Child sexual abuse images – the making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978.
- Grooming, incitement, arrangement or facilitation of sexual acts against children. Contrary to the Sexual Offences Act 2003.
- Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character). Contrary to the Criminal Justice and Immigration Act 2008.
- Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation). Contrary to the Public Order Act 1986.
- pornography;
- promotion of any kind of discrimination;
- threatening behaviour, including promotion of physical violence or mental harm;
- any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute;
- using school systems to run a private business;
- using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school;
- infringing copyright;
- revealing or publicising confidential or proprietary information (e.g. financial/personal information, databases, computer/network access codes and passwords);
- creating or propagating computer viruses or other harmful files;
- unfair usage (downloading/uploading large files that hinders others in their use of the internet);
- online gaming (non-educational);
- online gambling;
- personal online shopping/commerce;
- use of personal social media;
- use of messaging apps for personal use.

5.9 Cyber-bullying

Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will discuss cyber-bullying with their tutor groups, and the issue will be addressed in assemblies.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see the school Safeguarding Policy for more detail).

The school also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained. The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

5.10 Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities.

- Illegal Incidents - If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity report immediately to the police.
- Other Incidents - It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.

- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should 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 (except in the case of images of child sexual abuse – see below)
- 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 or national / local organisation (as relevant).
    - Police involvement and/or action.
    - If content being reviewed includes images of Child abuse then the monitoring should be halted and referred to the Police immediately.
- Other instances to report to the police would include:
    - incidents of 'grooming' behaviour;
    - the sending of obscene materials to a child;
    - adult material which potentially breaches the Obscene Publications Act;
    - criminally racist material;
    - other criminal conduct, activity or materials.
- Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the school for evidence and reference purposes.

6. Links with other policies

This online safety policy is linked to our:

- Child Protection and Safeguarding policy
- Good Behaviour policy
- Conduct and Discipline policy and procedure (staff)
- Data Protection (GDPR) policy and privacy notices
- Complaints and Resolution procedure
- Acceptable Use of Internet and Digital Technology policy
- HWCE Social Media Guidelines

Appendix 1: online safety Contacts and Resources

360 Safe Self-Review tool for schools

Action for Children

Action Fraud

Buckinghamshire Safeguarding Children Board

CEOP (Child Exploitation and Online Protection Centre)

ChildLine

Childnet

Get Safe Online

Internet Matters

IWF (Internet Watch Foundation)

Lucy Faithfull Foundation

The Marie Collins Foundation

NSPCC

Professional Online Safety Helpline

Thames Valley Police: in an emergency (a life is in danger or a crime in progress) dial 999. For other non-urgent enquiries dial 101 or use http://www.thamesvalley.police.uk/.

Think U Know

UKCIS (UK Council for Internet Safety)

UK Safer Internet Centre

Appendix 2: 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 up 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 / academy systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that parents and carers are aware of the importance of online safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

The school will try to ensure that *students / pupils* will have good access to digital technologies to enhance their learning and will, in return, expect the *students / pupils* to agree to be responsible users. A copy of the Student / Pupil Acceptable Use Policy is attached to this permission form, so that parents / carers will be aware of the school expectations of the young people in their care.

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

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PARENTS/CARERS

Parent / Carer Permission Form

Name of pupil:

Name of Parent/Carer:

As the parent / carer of the above *students / pupils*, I give permission for my son / daughter to have access to the internet and to ICT systems at school.

(KS2 and above)

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.

(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 Policy.

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.

Signed (parent/carer):	**Date:**

Appendix 2a: EYFS and KS1 acceptable use agreement (pupils and parents/carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS	
Name of pupil:	

When I use the school's ICT systems (like computers) and get onto the internet in school I will:
• Ask a teacher or adult if I can do so before using them
• Only use websites that a teacher or adult has told me or allowed me to use
• Tell my teacher immediately if:
  ○ I click on a website by mistake
  ○ I receive messages from people I don't know
  ○ I find anything that may upset or harm me or my friends
• Use school computers for school work only
• I will be kind to others and not upset or be rude to them
• Look after the school ICT equipment and tell a teacher straight away if something is broken or not working properly
• Only use the username and password I have been given
• Try my hardest to remember my username and password
• Never share my password with anyone, including my friends.
• Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carer
• Save my work on the school network
• Check with my teacher before I print anything
• Log off or shut down a computer when I have finished using it
I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.	

Signed (pupil):	**Date:**
Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Appendix 2b: KS2 acceptable use agreement (pupils and parents/carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS

Name of pupil:

I will read and follow the rules in the acceptable use agreement policy

When I use the school's ICT systems (like computers) and get onto the internet in school I will:

- Always use the school's ICT systems and the internet responsibly and for educational purposes only
- Only use them when a teacher is present, or with a teacher's permission
- Keep my username and passwords safe and not share these with others
- Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer
- Tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others
- Always log off or shut down a computer when I'm finished working on it

I will not:

- Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity
- Open any attachments in emails, or follow any links in emails, without first checking with a teacher
- Use any inappropriate language when communicating online, including in emails
- Log in to the school's network using someone else's details
- Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision

If I bring a personal mobile phone or other personal electronic device into school:

- I will not use it during lessons, tutor group time, clubs or other activities organised by the school, without a teacher's permission
- I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online
- I will hand it in to my class teacher/school office for safe-keeping whilst I am in school and will not use it whilst on school premises

I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.

Signed (pupil):	**Date:**

Parent/carer's agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.

Signed (parent/carer):	**Date:**

Appendix 2c: acceptable use agreement (staff, governors, volunteers and visitors)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS,VOLUNTEERS AND VISITORS	
Name of staff member/governor/volunteer/visitor:	
When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not: • Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material) • Use them in any way which could harm the school's reputation • Access social networking sites or chat rooms • Use any improper language when communicating online, including in emails or other messaging services • Install any unauthorised software, or connect unauthorised hardware or devices to the school's network • Share my password with others or log in to the school's network using someone else's details • Take photographs of pupils without checking with teachers first • Share confidential information about the school, its pupils or staff, or other members of the community • Access, modify or share data I'm not authorised to access, modify or share • Promote private businesses, unless that business is directly related to the school	
I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role. I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems. I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy. I will let the designated safeguarding lead (DSL) and Turn It On know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material. I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.	
Signed (staff member/governor/volunteer/visitor):	**Date:**

Appendix 3: Social Media Policy

Social media (e.g. Facebook, Twitter, LinkedIn) is a broad term for any kind of online platform which enables people to directly interact with each other. However some games, for example Minecraft or World of Warcraft and video sharing platforms such as YouTube have social media elements to them.

The school recognises the numerous benefits and opportunities which a social media presence offers. Staff, parents/carers and pupils/students are actively encouraged to find creative ways to use social media. However, there are some risks associated with social media use, especially around the issues of safeguarding, bullying and personal reputation. This policy aims to encourage the safe use of social media by *the school*, its staff, parents, carers and children.

Scope

This policy is subject to the school's Codes of Conduct and Acceptable Use Agreements.

This policy:

- **Applies to all staff and to all online communications which directly or indirectly, represent the school.**
- **Applies to such online communications posted at any time and from anywhere.**
- Encourages the safe and responsible use of social media through training and education
- *Defines the monitoring of public social media activity pertaining to the school*

The school respects privacy and understands that staff and pupils/students may use social media forums in their private lives. However, personal communications likely to have a negative impact on professional standards and/or the school's reputation are within the scope of this policy.

Professional communications are those made through official channels, posted on a school account or using the school's name. All professional communications are within the scope of this policy.

Personal communications are those made via a personal social media account. In all cases, where a personal account is used which associates itself with the school 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.

Digital communications with pupils/students are also considered. *Staff may use social media to communicate with learners via a school social media account for teaching and learning purposes but must consider whether this is appropriate and consider the potential implications.*

Organisational control – Roles & Responsibilities

SLT

- Facilitating training and guidance on Social Media use.
- Developing and implementing the Social Media policy
- Taking a lead role in investigating any reported incidents.

- Making an initial assessment when an incident is reported and involving appropriate staff and external agencies as required.
- Receive completed applications for Social Media accounts
- Approve account creation

Administrator / Moderator

- Create the account following SLT approval
- Store account details, including passwords securely
- Be involved in monitoring and contributing to the account
- Control the process for managing an account after the lead staff member has left the organisation (closing or transferring)

Staff

- Know the contents of and ensure that any use of social media is carried out in line with this and other relevant policies
- Attending appropriate training
- Regularly monitoring, updating and managing content he/she has posted via school accounts
- Adding an appropriate disclaimer to personal accounts when naming the school

Process for creating new accounts

The school community is encouraged to consider if a social media account will help them in their work, e.g. a history department Twitter account, or a "Friends of the school" Facebook page. Anyone wishing to create such an account must present a business case to the School Leadership Team which covers the following points:

- the aim of the account;
- the intended audience;
- how the account will be promoted;
- who will run the account (at least two staff members should be named);
- will the account be open or private/closed.

Following consideration by the SLT an application will be approved or rejected. In all cases, the SLT must be satisfied that anyone running a social media account on behalf of the school has read and understood this policy and received appropriate training. This also applies to anyone who is not directly employed by the school, including volunteers or parents.

Monitoring

School accounts must be monitored regularly and frequently (preferably 7 days a week, including during holidays). Any comments, queries or complaints made through those accounts must be responded to within 24 hours (or on the next working day if received at a weekend) even if the response is only to acknowledge receipt. Regular monitoring and intervention is essential in case a situation arises where bullying or any other inappropriate behaviour arises on a school social media account.

Behaviour

- **The school requires that all users using social media adhere to the standard of behaviour as set out in this policy and other relevant policies.**
- **Digital communications by staff must be professional and respectful at all times and in accordance with this policy**. Staff will not use social media to infringe on the rights and

privacy of others or make ill-considered comments or judgments about staff. School social media accounts must not be used for personal gain. Staff must ensure that confidentiality is maintained on social media even after they leave the employment of the school.

- Users must declare who they are in social media posts or accounts. Anonymous posts are discouraged in relation to school activity.
- If a journalist makes contact about posts made using social media staff must follow the school media policy before responding.
- Unacceptable conduct, (e.g. defamatory, discriminatory, offensive, harassing content or a breach of data protection, confidentiality, copyright) will be considered extremely seriously by the school and will be reported as soon as possible to a relevant senior member of staff, and escalated where appropriate.
- The use of social media by staff while at work may be monitored, in line with school policies. *The school permits reasonable and appropriate access to private social media sites. However, where excessive use is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken*
- The school will take appropriate action in the event of breaches of the social media policy. Where conduct is found to be unacceptable, the school will deal with the matter internally. Where conduct is considered illegal, the school will report the matter to the police and other relevant external agencies, and may take action according to the disciplinary policy.

Legal considerations

- **Users of social media should consider the copyright of the content they are sharing and, where necessary, should seek permission from the copyright holder before sharing.**
- **Users must ensure that their use of social media does not infringe upon relevant data protection laws, or breach confidentiality.**

Handling abuse

- When acting on behalf of the school, handle offensive comments swiftly and with sensitivity.
- If a conversation turns and becomes offensive or unacceptable, school users should block, report or delete other users or their comments/posts and should inform the audience exactly why the action was taken
- If you feel that you or someone else is subject to abuse by colleagues through use of a social networking site, then this action must be reported using the agreed school protocols.

Tone

The tone of content published on social media should be appropriate to the audience, whilst retaining appropriate levels of professional standards. Key words to consider when composing messages are:

- Engaging
- Conversational
- Informative
- Friendly (on certain platforms, e.g. Facebook)

Use of images

School use of images can be assumed to be acceptable, providing the following guidelines are strictly adhered to.

- **Permission to use any photos or video recordings should be sought in line with the school's GDPR Policy**. If anyone, for any reason, asks not to be filmed or photographed then their wishes should be respected.
- **Under no circumstances should staff share or upload student pictures online other than via school owned social media accounts.**
- Staff should exercise their professional judgement about whether an image is appropriate to share on school social media accounts. Students should be appropriately dressed, not be subject to ridicule and must not be on any school list of children whose images must not be published.
- If a member of staff inadvertently takes a compromising picture which could be misconstrued or misused, they must delete it immediately.

Personal use

- **Staff**
  - Personal communications are those made via a personal social media account. In all cases, where a personal account is used which associates itself with the school 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 private social media sites.*
- **Pupil/Students**
  - **Staff are not permitted to follow or engage with current or prior pupils/students of the school on any personal social media network account.**
  - The school's education programme should enable the pupils/students to be safe and responsible users of social media.
  - Pupils/students are encouraged to comment or post appropriately about the school. Any offensive or inappropriate comments will be resolved by the use of the school's behaviour policy.
- **Parents/Carers**
  - **If parents/carers have access to a school learning platform where posting or commenting is enabled, parents/carers will be informed about acceptable use.**
  - The school has an active parent/carer education programme which supports the safe and positive use of social media. This includes information on the website.
  - Parents/Carers are encouraged to comment or post appropriately about the school. In the event of any offensive or inappropriate comments being made, the school will ask the parent/carer to remove the post and invite them to discuss the issues in person. If necessary, refer parents to the school's complaints procedures.

Monitoring posts about the school

- As part of active social media engagement, it is considered good practice to pro-actively monitor the internet for public postings about the school.
- The school should effectively respond to social media comments made by others in a professional manner.

Appendix

When managing your personal use of Social Media, remember:

- "Nothing" on social media is truly private.
- Social media can blur the lines between your professional and private life. Don't use the school logo and/or branding on personal accounts.
- Check your settings regularly and test your privacy.
- Keep an eye on your digital footprint.
- Keep your personal information private.
- Regularly review your connections – keep them to those you want to be connected to.
- When posting online consider; Scale, Audience and Permanency of what you post.
- If you want to criticise, do it politely.
- Take control of your images – do you want to be tagged in an image? What would children or parents say about you if they could see your images?
- Know how to report a problem.

Managing school social media accounts

The Do's:

- Check with a senior leader before publishing content that may have controversial implications for the school.
- Use a disclaimer when expressing personal views.
- Make it clear who is posting content.
- Use an appropriate and professional tone.
- Be respectful to all parties.
- Ensure you have permission to 'share' other peoples' materials and acknowledge the author.
- Express opinions but do so in a balanced and measured manner.
- Think before responding to comments and, when in doubt, get a second opinion.
- Seek advice and report any mistakes using the school's reporting process.
- Consider turning off tagging people in images where possible.

The Don'ts:

- Don't make comments, post content or link to materials that will bring the school into disrepute.
- Don't publish confidential or commercially sensitive material.
- Don't breach copyright, data protection or other relevant legislation.
- Consider the appropriateness of content for any audience of school accounts, and don't link to, embed or add potentially inappropriate content.
- Don't post derogatory, defamatory, offensive, harassing or discriminatory content.
- Don't use social media to air internal grievances.

Appendix 4: Online Safety Training Needs: Self Audit for Staff

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/volunteer:	**Date**:
Question	**Yes/No (add comments if necessary)**
Do you know the name of the person who has lead responsibility for online safety in school?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	