Online Safety Policy

(To be read in conjunction with other safeguarding policies)

Introduction

In today's society, children, young people and adults interact with technologies such as mobile phones, games consoles and the Internet on a daily basis and experience a wide range of opportunities, attitudes and situations. The exchange of ideas, social interaction and learning opportunities involved are greatly beneficial to all, but can occasionally place children, young people and adults in danger.

Online safety covers issues relating to children and young people as well as adults, and their safe use of the Internet, mobile phones, tablets and other electronic communications technologies, both in and out of school. It includes education for all members of the community on risks and responsibilities and is part of the 'duty of care' which applies to everyone working with children. It should be noted that the use of the term 'online safety' rather than 'e-Safety' reflects a widening range of issues associated with technology and a user's access to content, contact with others and behavioural issues and a move away from a focus as online safety as an ICT issue.

Children and young people are likely to encounter a range of risks online which can be summarised as:

	Commercial	**Aggressive**	**Sexual**	**Values**
Content - Child as recipient	· Advertising · Spam · Copyright · Sponsorship	· Violent content · Hateful Content	· Pornographic content · Unwelcome sexual comments	· Bias · Racist and extremist content · Misleading info/advice · Body image and self esteem · Distressing or offensive content
Contact - Child as participant	· Tracking · Harvesting · Sharing personal information	· Being bullied, harassed or stalked	· Meeting strangers · Grooming · Online Child Sexual Exploitation	· Self-harm and suicide · Unwelcome persuasions Grooming for extremism

Conduct – Child as actor	· Illegal downloading · Hacking · Gambling · Privacy · Copyright	· Bullying, harassing or stalking others	· Creating and uploading inappropriate or illegal content (including "sexting") · Unhealthy/ inappropriate sexual relationships · Child on child sexualised or harmful behaviour	· Providing misleading information and advice · Encouraging others to take risks online Sharing extremist views · Problematic Internet Use or "Addiction" · Plagiarism

Content adapted from EU Kids Online 2008

Online safety also forms an important part of the Computing curriculum programmes of study for children and highlights the importance for children to use technology safely and respectfully, understand how to keep personal information private and be able to identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies from an increasingly early age. Children need to learn digital literacy skills and to refine their own publishing and communications with others via the Internet.

Respect for copyright and intellectual property rights, and the correct use of published material should be taught. Critical awareness of the dangers and consequences of plagiarism, copyright, piracy, reliability and bias will need to be explored. Children will need to develop an understanding on how to become safe and responsible online or digital citizens. Whilst the Computing Curriculum will form an essential part of online safety education for children and young people, safe and responsible use of technologies must be embedded throughout the curriculum to ensure children develop the required range of digital literacy skills and online resilience to enable them to become safe and responsible internet users.

Online safety is an essential element of our school's safeguarding responsibilities and requires strategic oversight and ownership to be able to develop appropriate policies and procedures to protect and prepare all members of the community. The online safety agenda has shifted towards enabling children and young people to manage risk and requires a comprehensive and embedded curriculum which is adapted specifically to the needs and requirements of children and the school. Online safety is embedded throughout our school's safeguarding practice and is clearly identified as an issue for leaders and managers to consider and address.

Our online safety policy is interlinked with many different policies including the Child Protection/Safeguarding Policy, Anti-Bullying, Home School agreement, Behaviour and School Development Plan and relates to other policies including those for personal, social, citizenship and health education (PSHCE).

Aims

The purpose of Barmston Village 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 technology to ensure that our school is a safe and secure environment.
- Safeguard and protect all members of the school community online.
- Raise awareness with all members of the school community regarding the potential risks as well as benefits of technology.
- To 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, external contractors , 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 a work laptop or mobile phone.
- This policy must be read in conjunction with other relevant school policies including (but not limited to) safeguarding and child protection, anti-bullying, behaviour, data security, image use, Acceptable Use Policies, confidentiality, screening, searching and confiscation and relevant curriculum policies including computing, Personal Social Health and Education (PSHCE), Citizenship and Relationships and Sex Education (RSE).

Online Safety involves pupils, staff, governors and parents making best use of technology, information, training and this policy to create and maintain a safe online and ICT environment for Barmston Village Primary School. Our Online Safety Policy has been written by the school, following government guidance. It has been agreed by senior management and approved by governors.

- The school's Online Safety Lead is Mr Jack Cunningham.
- The Online Safety Governor is Mrs Julie Stevens.
- The Online Safety Policy and its implementation shall be reviewed annually.
- The School Designated Safeguarding Lead (DSL) is Mrs Sara Bainbridge (head teacher).

Roles and Responsibilities

The management or leadership team (including the Governing body) within a school or setting have statutory responsibilities for child protection, of which online safety is an essential element. 'Keeping children safe in education' (September 2018) highlights specific statutory responsibilities for Governing bodies and leaders regarding online safety:

- Safeguarding policies and procedures:
  - *"54. Governing bodies and proprietors should ensure there are appropriate policies and procedures in place in order for appropriate action to be taken in a timely manner to safeguard and promote children's welfare."* (p.16)
  - *"55. This should include:*
    - *an effective child protection policy; and*
    - *a staff behaviour policy (sometimes called the code of conduct) which should amongst other things include - acceptable use of technologies, staff/pupil relationships and communications including the use of social media."* (p.16)
- Online Safety:
  - *"84. As schools and colleges increasingly work online, it is essential that children are safeguarded from potentially harmful and inappropriate online material. As such, governing bodies and proprietors should ensure appropriate filters and appropriate monitoring systems are in place. Additional information to support governing bodies and proprietors keep their children safe online is provided in Annex C."* (p.22)
- Opportunities to teach safeguarding:
  - *"85. Governing bodies and proprietors should ensure children are taught about safeguarding, including online, through teaching and learning opportunities, as part of providing a broad and balanced curriculum."* (p.22)

The Online Safety Lead and leadership team will take steps to consider existing school/setting practice using

tools such as the 360 safe self-evaluation toolkit (www.360safe.org.uk) to ensure that they are aware of the settings current strengths and areas of improvement. It is therefore vital that the school and leadership team have a sound awareness of online safety issues, and fully understand the importance of having effective policies and procedures in place.

Governors

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

The role of the Online Safety Governor will include:

- Regular meetings with the Online Safety Lead.
- Regular monitoring of Online Safety Incident logs (appendix 3).
- Reporting to the Governors.

Head Teacher and Senior Leaders

The Head teacher is responsible for developing, owning and promoting the online safety vision and culture to all stakeholders in line with national and local best practice recommendations with appropriate support and consultation throughout the school community. This is done by supporting the online safety lead in the development of an online safety culture within the setting.

The role of the Head teacher will include:

- Ensuring there are appropriate and up-to-date policies and procedures regarding online safety.
- Ensuring that suitable, age-appropriate and relevant filtering is in place to protect children from inappropriate content (including extremist material) to meet the needs of the school community and ensuring that the filtering and 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 and provide guidance regarding safe appropriate communications.
- Ensuring that online safety is embedded using a progressive whole school cross-curriculum approach which enables all pupils to develop an age-appropriate understanding of online safety and the associated risks and safe behaviours.
- Taking responsibility for online safety incidents and liaising with external agencies as appropriate.
- Liase with online safety lead to regularly review online safety incident logs and use them to inform and shape future practice.
- Ensuring there are robust reporting channels for the school/setting community to access regarding online safety concerns, including internal, local and national support.
- Ensuring that appropriate risk assessments are undertaken regarding the safe use of technology, including ensuring the safe and responsible use of devices.
- Ensuring a member of the Governing Body is identified with a lead responsibility for supporting online safety.
- Ensuring that the Designated Safeguarding Lead (DSL) works in partnership with the online safety lead.
- 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 online safety Lead.
- Ensuring 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 to support those colleagues who take on important monitoring roles.
- To 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 Online Safety Lead

The school have appointed an Online Safety lead, who is responsible for coordinating the whole school's online safety approaches, supporting and raising awareness with the wider community, promoting a safe and responsible

online safety culture and acting alongside the Designated Safeguarding Lead (DSL), in an advisory capacity, to deal with online safety issues that arise.

The online safety lead is a member of the leadership team due to the requirements and expectations of the role (directing resources and advising/supporting other staff) and ensuring that online safety is given a whole school approach with a coordinated focus.

The role of the Online Safety Lead will include:

- Working with and support technical staff in monitoring the safety and security of schools systems and networks.
- Taking day-to-day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policy/documents.
- Ensuring that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- Providing training and advice for staff.
- Receiving and regularly reviewing online safety incident logs and using them to inform and shape future practice.
- Acting as a named point of contact on all online safety issues and liaising with other members of staff and agencies as appropriate.
- Keeping up-to-date with current research, legislation and trends.
- Coordinating participation in local and national events to promote positive online behaviour, e.g. Safer Internet Day.
- Ensuring that online safety is promoted to parents and carers and the wider community through a variety of channels and approaches.
- Working with the head teacher/DSL for data protection and data security to ensure that practice is in line with legislation.
- Maintaining an online safety incident log, through CPOMs, to record incidents and actions taken as part of the schools safeguarding recording structures and mechanisms.
- Monitoring the school's online safety incidents to identify gaps/trends and update the education response to reflect need and to report to the school management team, Governing Body and other agencies as appropriate.
- Reviewing and updating online safety policies, Acceptable Use Policies (AUPs) and other procedures on a regular basis (at least annually) with stakeholder input.
- Ensuring that online safety is integrated with other appropriate school policies and procedures.
- Leading an online safety team/group with input from all stakeholder groups.
- Meeting regularly with a governor with a lead responsibility for online safety.
- Making appropriate resources available to support the development of an online safety culture.

Online Safety Group

Our ICT Team meet half termly to discuss the development of ICT in the school. Once per term one of these meetings is dedicated specifically to the discussion of Online Safety. For these meetings the following people are in attendance:

- Designated Safeguarding Lead
- Online Safety Lead/Computing Subject Lead
- Technical staff e.g. Network Manager, IT Technicians
- Other members of the senior leadership team - where appropriate

Agenda and minutes are shared with of the Online Safety designated Governor. The group will report regularly to the governing body to help inform them of existing practice and localised concerns.

Technical Staff

Technical staff have an essential role to play in establishing and maintaining a safe online environment and culture within establishments. Staff with responsibility for the technical environment should work closely with the school leaders and online safety lead to provide expertise relating to educational use of ICT systems and also to ensure that learning opportunities are not unnecessarily restricted by technical safety measures.

Technical staff will need clear supervision and support in their roles by the leadership and management team (including safeguarding leads) and, along with all staff, will require regular training and professional opportunities to enable them to remain up-to-date with emerging online safety issues. Technical staff should be clear about the procedures they must follow if they discover, or suspect, online safety incidents through monitoring of network activity and the need for these issues to be escalated immediately to the DSL.

<u>The role of the Technical Staff will include:</u>

- 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 team.
- To ensure that suitable access controls and encryption is implemented to protect personal and sensitive information held on school-owned devices.
- Ensuring that the schools filtering policy is applied and updated on a regular basis and that responsibility for its implementation is shared with the online safety lead and Designated Safeguarding Lead.
- Ensuring that the use of the setting's network is regularly monitored in order that any deliberate or accidental misuse can be reported to the online safety lead and DSL.
- Report any breaches or concerns to the Designated Safeguarding Lead and leadership team and together ensure that they are recorded on the online safety Incident Log, 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.
- Providing technical support and perspective to the online safety lead 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 setting machines and portable devices.
- Ensure that appropriately strong passwords are applied and enforced for all but the youngest users.

Teaching and Learning - staff

Children will come into contact with a variety of staff throughout their time in education and staff in schools and settings are likely to be the first point of contact for online safety incidents, or to identify changes in behaviour that may indicate that an individual is at risk of harm from online safety issues. It is therefore essential that all staff have a good awareness of online safety issues, and know the appropriate procedures for escalating online safety incidents or concerns to the safeguarding lead. All members of staff must be made aware of the duty to respond, report and record safeguarding issues and therefore be aware of the schools procedures for managing on and offline safety disclosures or concerns.

<u>The key responsibilities for all members of staff are:</u>

- 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 online safety issues, and how they relate to the children in their care.
- Modelling good practice in using new and emerging technologies and demonstrating an emphasis on positive learning opportunities rather than focusing on negatives.
- Embedding online safety education in curriculum delivery wherever possible.
- Identifying individuals of concern, and taking appropriate action by working with the designated safeguarding lead.
- 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.
- Maintaining a professional level of conduct in their personal use of technology, both on and off site.
- Reading, agreeing and signing the relevant acceptable usage agreements annually.

Teaching and Learning - pupils

The essential role and responsibilities of children and young people in relation to online safety should not be underestimated. Children should be encouraged and empowered to develop safe and responsible online behaviours to enable them to manage and respond to online risks as they occur. Children and young people form an important part of policy development, especially with regards to safeguarding as if children feel that their views have been heard (and in turn can understand some of the issues affecting the decisions) then they may be more inclined to abide by them.

It should also be understood that children are more likely to be aware of and understand new develops within technology and may be able to provide our school with an excellent way of keeping up-to-date with the rapidly changing pace of development, especially within social media and the associated apps and games.

<u>The key responsibilities of children and young people are:</u>

- 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.*

Teaching and Learning - parents

Parents/carers play a crucial role in developing children's safe and responsible online behaviours. We believe we have a clear responsibility to work in partnership with families to raise awareness of online safety issues. Through this approach, parents/carers can help our school to reinforce online safety messages and promote and encourage safe online behaviours wherever and whenever, children use technology. A partnership approach will be established via a variety of approaches and strategies and our school will ensure that online safety messages are shared and promoted with parents through a variety of communication channels and events throughout the year, including:

- Anti-bullying day
- Safer Internet Day
- Annual Online Safety Workshops
- Cyber-bullying Day

<u>The key responsibilities of parents and carers are:</u>

- Reading 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 new and emerging technology.
- 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 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.

Inclusion

Through ICT we ensure that the school meets the needs of all, taking account of gender, ethnicity, culture, religion, language, sexual orientation, age, ability, disability and social circumstances. It is important that in our school we meet the diverse needs of pupils to ensure inclusion for all and that all pupils are prepared for full participation in a multi-ethnic society. We also measure and assess the impact regularly through meetings with our SEND Co-ordinator and individual teachers to ensure all children have equal access to ensure success in this subject.

Pupils are taught in all lessons to be critically aware of the materials/content they access online and are guided to validate the accuracy of information.

The Internet and the World Wide Web

The Internet/World Wide Web is an essential element for education and social interaction. Internet/World Wide Web 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 pupils with quality Internet/World Wide Web access as part of their learning experience. The school's internet access will be designed to enhance and extend education, opening up new opportunities and educating the children on how to be safe day to day online.

However, there are inappropriate and undesirable elements that must be managed:

- If staff or pupils discover unsuitable sites, the URL (address), time and content shall be reported to the teacher who will then report to the Head teacher, by recording the incident in an Online Safety Log, which will be stored on CPOMs and in the school office. The online safety Log will be reviewed termly by the online safety Lead.
- The school will ensure that the use of Internet-derived materials by staff and pupils complies with copyright law.
- Pupils will be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.
- The school will work in partnership with our IT provider (Connected IT) to ensure filtering systems are as effective as possible.
- Access levels to the internet will be reviewed to reflect the curriculum requirements and the age and ability of pupils.
- Pupils will use age and ability appropriate tools to search the Internet for content. A child friendly specific search engine (Kidrex – powered by Google) will be used on all pupil computers and user areas.
- 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.
- The school will ensure that the use of Internet-derived materials by staff and pupils complies with

copyright law and acknowledge the source of information.

- All members of staff are aware that they cannot rely on filtering alone to safeguard children and supervision, classroom management and education about safe and responsible use is essential.
- 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 use age appropriate search tools as decided by the school following an informed risk assessment to identify which tool best suits the needs of our community.
- The school will use the internet to enable pupils and staff to communicate and collaborate in a safe and secure environment.
- 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.
- 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 given clear objectives for Internet use and taught what use is acceptable and what is not. (Responsible use of the Internet – appendix 4)
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- As part of the computing curriculum, all year groups have online safety, digital literacy and PSHCE lessons that focus on different elements of staying safe online. These lessons include topics from how to use a search engine, digital footprints and cyber bullying.

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 supports 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 measure in place.

Authorised Internet Access

By explicitly authorising use of the school's Internet access, pupils, staff, governors and parents are provided with information relating to online safety and agree to its use:

- All staff must read and sign the Acceptable Usage Agreement (appendix 5) before using any school ICT resource.
- Parents will be informed that pupils will be provided with supervised Internet access and asked to sign and return a consent form for pupil access.
- Only authorised equipment, software and Internet access can be used within the school.

Email

Email is an essential method of communication for staff, parents and pupils. The implications of email use for the school need to be thought through and appropriate safety measures put in place. Unregulated email can provide routes to the school community that bypass the traditional school boundaries and therefore use of personal emails by staff for any official school business are not be permitted.

Email is a quick and easy method of communication, ensuring beneficial and appropriate usage is an important part of online safety:

- Pupils may only use school provided email accounts for educational purposes.
- All members of staff are provided with a specific school email address to use for any official communication.
- The use of personal email addresses by staff for any official school business is not permitted.
- 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 must only be sent using secure and encrypted methods.
- Members of the school community must immediately tell a designated member of staff if they receive offensive communication and this should be recorded in the school online safety incident log.
- Sensitive or personal information will only be shared via email in accordance with data protection legislation.
- Whole -class or group email addresses may be used for communication outside of the school.
- Access in school to external personal email accounts is not permitted.
- School email addresses and other official contact details will not be used for setting up personal social media accounts.
- Pupils may only use approved email accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive email.
- Pupils must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission.
- Whole-class or group email addresses should be used in school rather than individual addresses.
- Access in school to external personal email accounts is not allowed.
- Email sent to external organisations should be written carefully and authorised before sending, in the same way as a using Outlook.
- Chain letters, spam, advertising and all other emails from unknown sources will be deleted without opening or forwarding.

Security and passwords

Passwords should be changed regularly. The system will inform users when the password is to be changed. Pupils and staff should never share passwords, and staff must never let pupils use a staff logon. Staff must always 'lock' the PC if they are going to leave it unattended (the picture mute or picture freeze option on a projector will allow an image to remain on the screen and also allow a PC to be 'locked').

See Password Policy

Social Networking

We acknowledge that there are significant potential benefits for communication, engagement, collaboration and learning via the Internet and social media. However we also need recognise that there are several risks associated with users (staff, pupils and the wider school community) especially when accessing and handling information as part of official School business.

For responsible children and adults, social media provides easy to use, free facilities, although are often free due to advertising and some sites may be dubious in content. Pupils should be encouraged to think about the ease of uploading personal information to social media sites as well as being made aware of the associated benefits. Pupils should be made aware of the potential risks of social media such as advertising, scams, contact from strangers and the difficulty of removing an inappropriate image or information once published.

Expectations regarding safe and responsible use of social media will apply to all members of theSchool community 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, forums, bulletin boards, multiplayer online gaming, apps, video/photo sharing sites, chatrooms, instant messenger and many others.

- All members of the school community will be encouraged to use 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 school community.
- All members of the school community are advised not to publish specific and detailed private thoughts, concerns, pictures or messages on any social media services, especially content that may be considered threatening, hurtful or defamatory to others.
- The school will control pupils and staff access to social media and social networking sites whilst on site and using school provided devices and systems.
- The use of social networking applications during school hours for personal use is not permitted, except when office staff are updating parents about school information using the social media sites.
- Any concerns regarding the online conduct of any member of the school community on social media sites should be reported to the school leadership team and will be managed in accordance with existing school policies such as anti-bullying, allegations against staff, 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 accordance with the relevant school policies, such as anti-bullying, allegations against staff, behaviour and safeguarding/child protection.

<u>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:</u>

- Ensuring that personal information is not published.
- Training is provided including: 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.

<u>School staff should ensure that:</u>

- No reference should be made in social media to 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.

<u>Official school social media accounts should:</u>

- Have a process for approval by senior leaders.
- Have clear processes for the administration and monitoring of these accounts – involving at least two members of staff.
- Have a code of behaviour for users of the accounts, including systems for reporting and dealing with abuse and misuse – (social media policy).
- Have clear procedures for how incidents may be dealt with under school disciplinary procedures

<u>Personal Use:</u>

- Personal communications are those made via a personal social media accounts. 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.

Monitoring of Public Social Media

- As part of active social media engagement, it is considered good practice to proactively monitor the Internet for public postings about the school.
- The school should effectively respond to social media comments made by others according to a defined policy or process.
- The school's use of social media for professional purposes will be checked regularly by the senior risk officer and Online Safety Group to ensure compliance with the school policies.

Reporting
All breaches of the Online Safety Policy need to be recorded in the Online Safety reporting file on CPOMs. The details of the user, date and incident should be reported.

Incidents which may lead to child protection issues need to be passed on to the Designated Person immediately – it is their responsibility to decide on appropriate action not the class teacher's.

Incidents which are not child protection issues but may require Lead Teacher intervention (e.g. cyber bullying) should be reported to the Lead Teacher in the same day.

Allegations involving staff should be reported to the Head Teacher. If the allegation is one of abuse, then it should be handled according to the DFE document titled 'Dealing with allegations of abuse against teachers and other staff'. If necessary, the local authority's LADO should be informed.
Evidence of incidents must be preserved and retained.

The curriculum will cover how pupils should report incidents (e.g. CEOP button, trusted adult, Childline).

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 / Academy Group 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.
    - Promotion of terrorism or extremism. (See Anti-Radicalisation policy)
    - 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 safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

Mobile Phones

Many mobile phones have access to the Internet and picture and video messaging, and such technologies present opportunities for unrestricted access to the Internet and sharing of images. There are risks of mobile bullying or inappropriate contact:

- Pupils are not permitted to use or bring mobile phones or devices in school.
- The sending of abusive or inappropriate text messages is forbidden.
- Staff should always use the school phone to contact parents.
- Staffs, including students and visitors, are not permitted to access or use their mobile phones within the classroom. All staff, visitors and volunteers should ensure that their phones are stored safely away in lockers or the school office and only used in designated mobile phone areas.
- School mobile phones should be used when on school trips, not personal phones.
- Under no circumstances are photos to be taken of pupils using personal mobile phones.

Digital/Video Cameras/Photographs

When using digital images, staff should inform and educate students / pupils 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. Pictures, videos and sound are not directly connected to the Internet but images are easily transferred.

- Pupils will not use digital cameras or video equipment at school unless specifically authorised by staff.
- Publishing of images, video and sound will follow the policy set out in this document under 'Publishing Content'.
- Written permission from parents or carers will be obtained before photographs of students / pupils are published on the school website / social media / local press.
- Parents and carers are only permitted to take photos/videos of their own children at school events.
- The Head Teacher or a nominee will inform parent(s)/guardian(s) and others present at school events that photographs/videos of their own children will only be taken be not be taken during performances and not shared on any sort of social media.
- School devices and cameras should be logged accordingly to who they have been assigned to.
- See Photograph policy.

Staff should always use a school camera to capture images and should not use their personal devices.
Photos/videos should immediately be transferred from school devices to school staffshare and deleted from mobile devices.

Photos taken by the school are subject to the Data Protection Act.

Published Content and the School Website

The school website is a valuable source of information for parents and potential parents.

- Contact details on the website will be the school address, email and telephone number.
- Staff and pupils' personal information will not be published.
- The online safety lead and school bursar will take overall editorial responsibility and ensure that content is accurate and appropriate.
- Photographs and videos that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.
- Pupils' full names will not be used in association with photographs.
- Consent from parents will be obtained before photographs of pupils are published on the school website.
- Work will only be published with the permission of the pupil.
- Parents should only upload pictures of their own child/children onto social networking sites.
- The Governors may ban the use of photographic equipment by any parent who does not follow the school policy.

Information System Security

- 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 users will be provided with a username and secure password by the school technician who will keep an up to date record of users and their usernames. Staff are responsible for the security of their username and password and will be required to change their password regularly.
- The "master / administrator" passwords for the school ICT system, used by the Network Manager (or other person) must also be available to the Head teacher or other online safety lead and kept in a secure place (e.g. school safe).
- School bursar is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licenses purchased against the number of software installations (Inadequate licensing could cause the school to breach the Copyright Act which could result in fines or unexpected licensing costs).
- 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. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes see filtering policy for more details.
- Internet filtering should ensure that children are safe from terrorist and extremist material when accessing the internet. Nb. additional duties for schools under the Counter Terrorism and Securities Act 2015 which requires schools to ensure that children are safe from terrorist and extremist material on the internet.
- The school has provided enhanced / differentiated user-level filtering (allowing different filtering levels for different ages / stages and different groups of users –staff / pupils / students etc.)
- School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.
- An appropriate system is in place for users to report any actual /potential technical incident / security breach to the relevant person, as agreed).
- 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. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- An appropriate procedure is in place for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the school systems.

Protecting Personal Data

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 will 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.
- It has a Data Protection Policy.
- Risk assessments are carried out.
- It has clear and understood arrangements for the security, storage and transfer of personal data
- Data subjects have rights of access and there are clear procedures for this to be obtained.
- There are clear and understood policies and routines for the deletion and disposal of data.
- There is a policy for reporting, logging, managing and recovering from information risk incidents.
- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties.
- There are clear policies about the use of cloud storage / cloud computing which ensure that such data transfer / storage meets the requirements laid down by the Information Commissioner's Office.

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.
- The device must offer approved virus and malware checking software.
- The data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete.

Assessing Risk

The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school does not accept liability for the material accessed, or any consequences of Internet access. The school will audit ICT use to establish if the Online Safety Policy is adequate and that the implementation of the Online Safety Policy is appropriate.

Handling Online Safety Complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff.

- Any complaints about staff misuse must be referred to the Head Teacher.
- Complaints of a child protection nature shall be dealt with in accordance with school Child Protection procedures.
- Pupils and parents will be informed of the complaints procedure.
- Discussions will be held with the community police officer to establish procedures for handling potentially illegal issues.

Communication of Policies

It is important that all policies are shared with all members of the school community, in order to emphasise the importance of online safety in this day and age when technology is ever growing and playing a huge part in our daily lives.

Pupils:

- Rules for Internet access will be posted in all networked rooms.
- Pupils will be informed that Internet use will be monitored.
- Pupils will be informed of the importance of being safe on social networking sites such as MSN and Instagram. This will be strongly reinforced across all year groups during ICT lessons, and all year groups look at different areas of safety through the digital literacy lessons.

Staff:

- All staff will be given the school Online Safety Policy and its importance will be explained.
- Staff will be expected to sign annually.

Parents:

- Parents' attention will be drawn to the school Online Safety Policy in newsletters and on the school website.

Further Resources

We have found these web sites useful for online safety advice and information:

www.thinkuknow.co.uk	Set up by the police with lots of information for parents and staff, including a place to report abuse.
www.childnet-int.org	Non-profit organisation working with others to "help make the Internet a great and safe place for children".
www.saferinternet.org.uk	Safer Internet Centre – where you can find e-safety tips, advice and resources to help children and young people stay safe on the Internet.
www.ceop.police.uk	CEOP – protect children from harm online and offline, directly through NCA led operations and in partnership with local and international agencies.

Other documents to be read in conjunction with Online Safety Policy:

- Computing Policy
- Child Protection Policy

- Responsible Use of the Internet (pupil)
- Acceptable ICT Use Agreement (staff)
- Guide to safer working practice
- Photograph Policy
- Permission for photographs to be taken
- Anti-Radicalisation Policy
- Password policy
- Photograph Policy

Policy will be reviewed annually with staff and pupils where appropriate.