Online Safeguarding Policy

Revised Dec 2025

(Version 19)

Adapted from Sheffield Safeguarding Children Board

Contents

Policy Introduction and Rationale

Development, Monitoring and Review of the Policy

Monitoring and Communication

Roles and Responsibilities

The Curriculum

Using Digital and Video Images

Managing Internet Access, Security and Passwords

- System Security
- Content Filtering and Monitoring - Safeguarding
- Assessing Risks
- Setting Usernames and Passwords
- Internet Access
- Internet Use
- Handling Incidents
- E-mailing
- Social Networking – Pupils
- VOIP - Skype / Facetime
- Managing Technologies
- Google Education
- Cloud Computing
- School Website
- Twitter Usage

Protecting Personal Data and GDPR

Mobile Phones and Devices

Policy Introduction

This Online Safeguarding Policy is important to school for a number of reasons, including to:

- Ensure all members of the school community use technology safely, respectfully and responsibly; recognise acceptable/unacceptable behaviour; identify a range of ways to report concerns about content and contact.
- Ensure that everyone in the school community is fully aware of their role and responsibilities with regards to Online Safety.
- Ensure all members of the school community understand and respect boundaries for the use of school owned and personal technology used in the school.
- Understand the need to use online services responsibly and professionally including social media, communication and cloud storage platforms.
- Ensure all members are aware of the sharing and storing of personal data as part of the Protection of Personal Data and GDPR legislation.
- Ensure there is a clear and consistent approach when responding to any incidents.

Rationale

The children in today's society have the opportunity to access a wide range of new technologies including the internet, a variety of communication technologies and other digital media. Online Safety encompasses both Internet technologies and electronic communications. These are powerful and innovative tools which bring new opportunities for both teachers to teach and pupils to learn. Using such technologies promotes communication, discussion, thinking, creativity, can stimulate learning and even raise educational standards and achievement. However, in order to use these technologies effectively, we need to educate our children about the benefits and risks they may encounter whilst online. These risks can be categorised into three areas according to the document **Keeping Children Safe in Education (September 2021)**

Content: being exposed to illegal, inappropriate or harmful material; for example pornography, fake news, racist or radical and extremist views;

Contact: being subjected to harmful online interaction with other users; for example commercial advertising as well as adults posing as children or young adults; and

Conduct: personal online behaviour that increases the likelihood of, or causes, harm; for example making, sending and receiving explicit images, or online bullying

Commerce: risks such as online gambling**, inappropriate advertising, phishing** and or financial scams.

This Online Safety Policy will be used in conjunction with other policies embedded in school.

- Social Media Policy
- Acceptable Use Policies
- Behaviour Policy
- Anti-bullying Policy
- Safeguarding and Child Protection Policies
- Data Protection Policy

As a school our approach to Online Safety is to protect the whole school community. Therefore, at St Wilfrid's Primary School we have Acceptable Use Policies for the whole school community which have been created with Sheffield Catholic Schools Partnership.

Online Safety is embedded in school through a digital citizenship programme from Reception to Year 6 and is taught through PSHE, Computing, Assemblies and Themed Days/Weeks. It is impossible to remove all risk, however, we will endeavour to build our pupils resilience and information to the risks they may encounter when online, so that they have the confidence, power and skills to stay safe.

Incidents will be dealt with, whether in or out of school in accordance with this policy and the other policies mentioned above.

Development, Monitoring and Review

Title	**Online Safety Policy**
Version	19
Date	*Dec 2025*
Authors / Co-Authors	*Mrs Karen Sadler / Jane Corcoran*
This online Safety policy was approved by the Governing Body on*:*	
The policy has been read and agreed by staff. Staff have signed the Workforce Acceptable Use Policy	Online Google Form
Monitoring will take place at regular intervals (at least annually):	by Mrs J Corcoran and then Senior Leadership Team
The Governing Body will receive a report on the implementation of the policy including anonymous details of any online Safety incidents at regular intervals:	Every term alongside the termly Safeguarding Report from the Head Teacher.
The Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online Safety or incidents that have taken place. The next anticipated review date will be:	*Dec 2026*
Should serious online safety incidents take place, the following persons / agencies should be informed:	*Follow Procedures within Safeguarding Policy*

Monitoring

This online Safety policy is developed and then monitored by Mrs Jane Corcoran with support from the Online Safety Team on an annual basis, or as events change or as a result of an incident taking place. The Online Safeguarding Team for each school includes: the Headteacher, the Designated Safeguarding Lead/ Deputy, Computing Subject Leader/Online Safety Co-ordinator, PSHE Subject Leader and Governors.

The school will monitor the impact of the policy using:

- Monitoring of pupil activity during lesson times
- Logs of reported incidents in CPOMS
- Parents and pupils views regarding online Safety
- Questionnaires
- If an incident occurs where teaching and learning is impacted (Eg Covid 19)

Communication of this Policy

All school community members will receive the appropriate Acceptable Use Policy. They will be informed that all internet use in school maybe monitored and traced to the individual and therefore appropriate conduct must be adhered to at all times.

Communication of this policy for the school workforce, parents/carers and pupils will take place in a variety of ways.

School Workforce

- All amendments will be published and where appropriate awareness sessions will be held.
- Regular staff training of awareness and any updates through staff/governor meetings or INSET

Parents/Carers

- Parent workshops to be delivered and ongoing communication via the school's systems. Attention will be drawn to online Safety in newsletters, blogs and the school website.
- Support will be provided to ensure parents/carers promote the positive use of the internet and social media

Pupils

- Rules for online Safety and internet use are posted around the school.
- Online Safety updates will be included in the curriculum to ensure pupils are aware of any updates and risks.

Roles and Responsibilities

We believe that online Safety is the responsibility of the whole school community.

Senior Leadership:

- The Headteacher has overall responsibility for the online safety of all members of the school community.
- The Headteacher and senior leadership team are responsible for ensuring that the Safeguarding Lead and other relevant staff receive suitable training to enable them to carry out their role and to train other colleagues when necessary.
- Monitors the recording of incidents within school and also monitors the filtering process in school through regular reports being sent to safeguarding@stwilfridssheffield.co.uk.
- The Head Teacher and Safeguarding Lead should be aware of procedures to be followed in the event of a serious incident or allegation being made with regards to online safety and they should be aware of procedures to be followed. (follow safeguarding policy)

Governors:

- Provide a designated Online Safety Governor to support the Online Safety Subject Leader in school.
- Approve and monitor the Online Safety Policy. Information will be given about all logged incidents from the Head Teacher's Report.
- Read, understand, contribute to and help promote the school's Online Safety and Acceptable Use Policies.
- Develop an overview of how the school infrastructure provides safe access to the internet.
- Know how the school encourages pupils to adopt safe and responsible behaviours in their use of technology in and out of school.
- Support the work of the Online Safety Team in promoting and ensuring safe and responsible use of technology and platforms in and out of school.
- Ensure appropriate funding and resources are available for the school to implement its Online Safety strategy.

Online Safety Team

- Ensures that the school online Safety policy is current and systematically reviewed
- Ensures that school Acceptable Use Policies are appropriate for the intended audience.
- Promotes to all members of the school community the safe use of the internet and any technologies deployed within school.
- Ensures the school is aware of the procedures that need to take place in the event of any online Safety incident occurring in school.

Safeguarding Lead:

- Takes day-to-day responsibility for online Safety within school.
- Has regular contact with other online Safety committees including Sheffield Safeguarding Children Board.
- Monitors any online Safety incidents that have been recorded.
- Understands the issues surrounding the sharing of personal or sensitive information.
- Understands the dangers regarding access to inappropriate online contact with adults and strangers.
- Is aware of potential or actual incidents involving grooming of young children.
- Is aware of and understand cyberbullying and the use of social media for this purpose.

Online Safety Subject Leader:

- Promotes an awareness and commitment to online Safety throughout the school.
- Takes a leading role in establishing and reviewing the school online Safety policies and procedures.
- Leads the school online Safety group.
- Attends regular training to keep updated.
- Provides necessary training and support to staff.
- Liaises with other outside agencies when necessary, including the LA and Community Police.
- Communicates with school technical staff and with the designated online Safety governor.
- Develops an understanding of current online Safety issues, guidance and appropriate legislation.
- Ensures that online Safety is embedded across the curriculum.
- Ensures that online Safety is promoted to parents and carers.
- Monitors and reports on online Safety issues to the online Safety group and the senior leadership team as appropriate.
- Ensures that all staff are aware of the procedures that need to be followed in the event of an online Safety incident.
- Ensures that an online Safety incident log is kept up to date.

Staff:

- Read, understand and help promote the school's online Safety policies and guidance.
- Read, understand and adhere to the school School Workforce Acceptable Use and Social Media Policies.
- Report any incidents or misbehaviour with regards to online Safety to the online Safety leader or safeguarding team.
- Models safe and responsible behaviours in their own use of technology.

- Ensure that any digital communications with pupils should be on a professional level and only through school-based systems, NEVER through personal mechanisms, e.g. personal email addresses, texts or mobile phones.
- Implements the school online Safety policy and curriculum framework.
- Deliver online Safety objectives in all aspects of the school curriculum, including computing, PSHE lessons, in antibullying week and Internet Safety Day/Week.
- Ensure the children understand and follow their Pupil Acceptable Use Policy
- Supervise ICT activities in school and ensure activities are focussed with clear pre-planned tasks to guide the children when on the internet
- Staff must use cloud storage or encrypted sticks for handling school data and school based digital cameras, devices and mobile phones for taking images and videos. Staff need to implement these rules on and off site.
- Staff must ensure all personal devices, including phones and tablets are stored out of sight of children during lesson time.
- Create an environment where children know what to do if inappropriate material is discovered on the internet or if they feel threatened or uncomfortable with any form of online communication.
- Ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws.
- Ensure volunteers working alongside them adhere to the School Worksforce Acceptable Use Policy
- Understand and be aware of incident-reporting mechanisms that exist within the school.

Technical Staff: (Notre Dame High School IT Technicians)

- Take responsibility for the security of the school ICT infrastructure and systems
- Manage content filtering and follows information that the Local Authority gives as guidance to maintain the school's systems and firewall.
- Ensure passwords are secure, updated and changed when necessary.
- Ensure software (including antivirus software) is regularly updated.
- Liaise with appropriate people and organisations on technical issues.
- Restrict all administrator level accounts appropriately.
- Ensure that access controls exist to protect personal and sensitive information held on school-owned devices.
- Ensure that appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster.

The Curriculum

- The SMART rules will be on display in all classrooms and are reinforced during session time.
- Children will be continually encouraged during Computing and PSHE sessions to think about online Safety.
- The Online Safety Curriculum Framework will be used as guidance to support appropriate activities and objectives the pupils need to cover.
- Online Safety is also promoted through planned assemblies and during specific days and weeks like Anti-Bullying week and National Internet Safety Day. Activities will include using sites like the Think U Know website at www.thinkuknow.co.uk from the Child Exploitation and Online Protection Centre (CEOP) and the Childnet International site at http://www.childnet-int.org/.
- We will discuss, remind or raise relevant Online Safety messages with pupils routinely wherever suitable opportunities arise during all lessons; including the need to protect personal information and to consider the consequences their actions may have on others.
- Internet use is carefully planned and learners are guided to web sites which are age appropriate and support the learning objectives for specific areas of the curriculum.
- We will teach pupils how to use search engines appropriately to search for information and to evaluate the content of websites for reliability, including fake news.
- Children are taught what to do if inappropriate content is found during searches. Staff should be vigilant at all times when learners are searching.
- Learners are taught to be aware of the materials they access and to think about how to validate the accuracy of the information they find.
- Plagiarism and copyright laws are reinforced and the children are taught how to acknowledge materials used from the Internet.
- Pupils will be taught about the impact of cyberbullying and know how to seek help if they are affected by any form of online bullying.
- Pupils will be made aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent or carer, teacher or trusted staff member, or an organisation such as Childline or the CEOP report abuse button.

Using Digital and Video Images

(Taking Photographs at School Events)

All members of the school community need to be aware of the risks associated with the sharing and posting of digital images on the Internet and the potential implications for their future. Therefore it is important that we as educators take the following actions:

- Teach our members the risks associated with the taking, sharing and distribution of images. For example, on social networking sites, they are on view to potential employers (cyber vetting) and potential groomers. We need to teach all school members about their digital footprint and the risks attached with publishing their own images.

- Staff to plan the photographs they take for educational purposes and ensure pupils are appropriately dressed. We need to ensure we have parental consent to use or publish those images. Images should only be taken on school equipment, use of personal equipment needs to be authorised by the head teacher.

- Learners are taught not to upload, share or distribute images of themselves or others to the internet without seeking permission. Educational Videos like “Think Before You Post” (by CEOP) will be viewed to get this message across.

- Students’ / Pupils’ full names will not be used anywhere on a website or blog, particularly in association with photographs.

- Written permission from parents or carers will be obtained before photographs of students / pupils are published on the school website, prospectus etc. (see form in appendix)

Managing Internet Access and Security

Pupils will continue to use the Internet outside school and so will need to learn how to *"use technology safely, respectfully and responsibly; recognise acceptable/unacceptable behaviour; identify a range of ways to report concerns about content and contact."* (Computing Programmes of Study)

As a school it is our role to ensure pupils can balance the benefits of using the internet with an awareness of the potential risks.

System Security

- Users need to seek advice and permission from the school technical team before downloading any programs. An administration code is required.
- The school IT systems capacity and security will be reviewed regularly by the schools technical team.
- Virus protection is installed and updated regularly by the school technical team on all workstations within the infrastructure.

Content Filtering and Monitoring – Safeguarding

We use Smoothwall Web Filtering Solution. This incorporates a firewall to protect the school's network from external hackers. It also monitors web use and can flag up web search terms that may give cause for concern. The school has more control and additional features to filtering. Filtering is done locally in school which means we have control on what is blocked and unblocked. The Smoothwall devices also have advanced features that allow monitoring of web use.

Filtering policies have been set up for different users in school. For example, teachers have more access than pupils to content like You Tube and Social Media. Therefore it is paramount that teachers check the content the pupils will see before the lesson starts to ensure it is safe.

There is a safeguarding suite feature which allows us to monitor search terms entered and flagged in the categories of:
Radicalisation, Suicide, Abuse, Substance Abuse, Bullying, Criminal Activity and Adult Content.

When one of these flags is triggered the system administrator is provided with a report which the SLT can use as evidence in dealing with the incident. The colours Red, Yellow and Blue are used to label the seriousness of the incident. An email has been set up (safeguarding@stwilfridssheffield.co.uk) to receive weekly/monthly reports, which should be monitored by the safeguarding team.

Groups of vulnerable children may be set up on the system in order to run a report on these children.

- The school will always be proactive regarding the nature of content which can be viewed.
- The school will have a clearly defined procedure for reporting breaches of filtering. All staff and pupils will be aware of this procedure by reading and signing the Acceptable Use Policy
- If users discover a website with inappropriate content, this should be reported to a member of staff who will inform the Online Safety Subject Leader and Technical Team.
- All incidents should be documented.
- If users discover a website with potentially illegal content, this should be reported immediately to the Online Safety Subject Leader or SLT. The school will report such incidents to appropriate agencies including the filtering provider.
- The school will regularly review the filtering product for its effectiveness.
- Any amendments to the school filtering or block-and-allow lists will be checked and assessed prior to being released or blocked through the school's technician or online Safety subject leader.
- Pupils will be taught to assess content as their internet usage skills develop.
- Levels of internet access and supervision within our school may well vary depending on the user. Pupils and Teachers may have different filtering policies applied to their internet use, either temporarily or permanently as we have moved towards a less locked down service.

Assessing Risks

- 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 cannot accept liability for the material accessed, or any consequences of Internet access.

Setting Usernames and Passwords

- A secure username and password convention exists for all system access. The technicians can access all equipment including resetting users passwords when necessary.
- Key Stage 1 pupils will have a generic 'pupil' logon to all school ICT equipment.
- Pupils at Key Stage 2 are moving towards individually-named user account and password for access to ICT equipment.
- All staff will have a unique, individually-named user account and password for access to ICT equipment and information systems available within school.
- Users should change their passwords at prearranged intervals (every 6 weeks) or at any time that they feel their password may have been compromised.
- All staff and pupils have a responsibility for the security of their username and password.
- Users must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- Only disclose your personal password to authorised IT support staff when necessary and never to anyone else. All personal passwords that have been disclosed should be changed as soon as possible.
- Never display, write down or save system-based usernames and passwords within an internet browser where it asks the user to save their password.
- All access to school information assets will be controlled via username and password.
- No user should be able to access another user's files unless delegated permission has been granted.
- Users must not attempt to impersonate anyone else.
- The user must not leave their PC unlocked and ensure they lock their device before leaving it unattended. This is essential during wet break and lunchtimes when pupils could gain access.
- Users should create different passwords for different accounts and applications.
- Users should use 8 characters including numbers, letters and special characters in their passwords to ensure they are strong enough (! @ # $ % *)

Internet Access

- Pupils and Staff will discuss and sign the Acceptable Use Policy to know what Internet use is acceptable.
- When a member of the school community departs from the school the technical team must ensure any user information held by this member has been deleted to safe guard children and school data. This includes google accounts and access to the online community.
- Any visitors who are with the school for a period of time must also agree to the Acceptable Use Policy relevant to them.
- Parents will be informed that pupils will be provided with supervised Internet access and will be asked to read the Acceptable Use Policy with their child. If they disagree it is the parent's responsibility to inform the school. (This information will be included in all new pupils starter packs)

Internet Use

- Staff should guide pupils in on-line activities that will support learning outcomes planned for the pupils' age and maturity.
- Pupils should always be supervised when using computers and tasks that are set are focussed and within the curriculum or to support any learning taking place.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- School will ensure that the use of Internet derived materials by pupils and staff complies with copyright law.
- Pupils should be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.

Handling Incidents – (follow safeguarding policy)

- Internet misuse will be dealt with and sanctions given by the class teacher at the time of the misuse.
- Incidents will be reported to the Online Safety Coordinator/Safeguarding Lead/ The Head Teacher who will judge whether it is necessary to just log the incident, or inform the Sheffield Safeguarding Team or/and the police.
- If misuse is repeated, Parents will be informed.
- Any complaint about staff misuse will be referred immediately to the Head Teacher and discussions with the local police if appropriate.
- Complaints of a child protection nature must be dealt with in accordance with school child protection and safeguarding procedures.
- Illegal issues with be handled through discussions with the Head Teacher, safeguarding Lead, Governor Representative and Local Police.

Emailing

- Pupils/staff must immediately tell a teacher/head teacher if they receive offensive or any unknown external e-mail within their own or group accounts.
- Pupils must not reveal personal details of themselves (including their e-mail address) or give information of other peoples details in e-mail communication, or arrange to meet anyone without specific permission.
- Any e-mail in school should only be sent through approved email accounts setup by the class teacher. Pupils must have permission before emailing in school. The passwords on these accounts can be changed by the teacher after the session if so required.

Social Networking Sites - Pupils

- The School uses Smoothwall Firewall which blocks/filters/monitors access to social media sites unless a specific use is approved.
- Pupils are advised to only use moderated sites specifically for their age group and to seek consent from an adult.
- Pupils are advised never to give out personal details or complete online forms of any kind which may identify them or their location
- Pupils are advised not to upload personal photos of themselves or others on any social network space without permission.
- Pupils are advised on security and encouraged to set ‘strong’ passwords, deny access to unknown individuals and instructed how to block unwanted communications.
- Pupils are encouraged to use privacy settings and invite known friends only and deny access to others if such sites were to be used.

VOIP – Skype / Facetime / Google Meet

- VOIP if used, will only be used in a teacher directed and supervised environment.
- Staff have the responsibility to ensure the connection is closed on the device after use.

Managing Technologies (Netbooks, Tablets, Cameras, Mobile Phones)

- Emerging technologies will be examined for educational benefit and a risk assessment will be discussed by the Online Safety team before use in school is allowed.
- All equipment in school is to support the education and wellbeing of our children.
- Focussed tasks will be provided to the children when allowed on any of these emerging technologies and boundaries set by the teacher.

Google Education - GSuite for Education Apps

Staff Users

- Staff members use GSuite Education apps for communication and sharing purposes.
- Staff use google email, calendars and drive
- Any personal data relating to staff or pupils is minimal on these platforms
- Only initials or first names of the children are used
- There are no advertisements used with Google Apps for Education. Additional information on google security and filtering can be found at:
- http://www.google.com/support/a/bin/answer.py?answer=60762
- http://www.google.com/support/a/bin/answer.py?answer=60730

Pupil Users (See Google Classroom and Google Meet Rules)

- All pupils have Google Classroom Accounts for remote access and for computing lessons.
- Applications are switched on and off when needed by the administrator.
- Pupils need to follow the Google Classroom and Google Meet Rules when using these applications.

Cloud Hosted Services

The UK Government and the Information Commissioner's Office have issued guidance about the use of 'Cloud'.

https://ico.org.uk/media/for-organisations/documents/1540/cloud_computing_guidance_for_organisations.pdf

- The school will approve any use of Cloud Computing for sharing information and collaborating. This maybe through Google Drive, Dropbox or IRIS (**Institutional Research Information Service** and is a one-stop shop for information on research activity at UCL where the Maths Mastery Project is based which we follow in school.

- Users must not store any sensitive information in the Cloud which has not been formally assessed and approved by the school.

Enabling home-based working for staff & pupils

- If staff use their personal devices, they will need to seek permission from the headteacher.
- No pupil information should be downloaded and kept on personal devices after the completion of the session.
- Staff must not use social media apps with pupils.
- Staff should not set up their own systems of communication with pupils. The method chosen by the school and should be approved by the Headteacher (We use Google Classroom for Communication with Pupils)

Enabling pupils to work from home

If pupils are being asked to share photos of their work with their teacher, the teacher should remind them about key messages around online Safety and the school's usual policy around photographs should apply. The school's online Safety coordinator should be consulted for advice.

Video Calling – Google Meet and School Cloud (See Google Meet Rules and Permission Form)

At St Wilfrid's video conference platforms are used for remote learning sessions and parents meetings. We require parental involvement in the video call to ensure adult supervision is always there.

- Staff should only use generic school-based accounts and apps to communicate with pupils. Under no circumstances should they use their personal accounts for this work.
- If you are holding video conferencing live sessions with pupils of any age, this must be with parental permission and with the approval of the Headteacher. It is good practice to have at least two adults in the conference at any one time.
- For one-to-one sessions (e.g. music tuition), staff must have the express permission of the headteacher and parent.
- Parental permission should take the form of a virtual hello at the start of the session and a virtual goodbye at the end of the session. There is no need for the parent to be present for the whole of the session.
- Teachers and pupils should be appropriately dressed and in a living space, i.e. not a bedroom.
- Background noise interference can be removed by muting microphones for all but the current speaker.

School Website (See Separate Website Policy)

- The school's online community is developed and updated by its school members who ensure that content is accurate, up to date and safe for public access.
- Contact details include the school address, e-mail and telephone number. Staff or pupils personal information will not be published without consent.
- It is a communication tool used for pupils, parents and staff of the school. The public can access the site to find out about the school and to share its successes.
- Blogs are an everyday part of the site and through online Safety training with our pupils and monitoring we ensure the blogs are safe to view.
- This online community helps us to prepare our children for the safe use of the internet when they are in and out of school.

Twitter Usage

Schools around the world are using Twitter which means that children's great work can be published and teachers can collaborate. To ensure appropriate online Safety measures are in place, the school regulates who is able to 'follow' us on Twitter and no full names of children are included. Obviously any image posted online is in the public domain, which is why we take sensible measures.

.

Twitter is used by school staff to communicate with parents and education places the following:

- children's achievements, successes and school/national updates.
- safe and responsible use of technology and social media.
- encourage the use of 21st Century technology

Twitter accounts will:

- Only follow educationally linked accounts. No personal accounts, unless they are educationally linked, will be followed.
- Not reply to any 'replies' on Twitter. This is not the platform to discuss or debate school related issues.
- Only use children's first names if referencing children and images will be checked according to the digital image policy
- Use Twitter to share positive messages about the school.

Parents and staff use of Twitter should be in line with the school's Social Media and Acceptable Use Policies.

Protecting Personal Data
(See Data Protection Policy and Privacy Notices for further Details)

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.

See the Information Commissions Office for further guidance:
https://ico.org.uk/for-organisations/guide-to-data-protection/

All staff in school must ensure:

- They take care and safe of all personal data, minimising the risk of its loss or misuse.
- They send personal data securely off the school site. (See School Business Manager)
- Use password protected computers and ensure equipment is logged-off at the end of the session where personal information could be accessed or viewed.
- Transfer or store data using encrypted and secure password devices.
- Any data transferred is used on a virus protected system which is regularly updated.
- All data is deleted from the device once transfer is complete.
- Digital Cameras are cleared before allowing off site and photographs are transferred to the school protected systems.
- Equipment that is taken off site must be checked that no personal information can be accessed.
- All devices taken off site, e.g. laptops, tablets, removable media or phones, need to be secure in a locked, safe environment and, for example, not left in cars or insecure locations.

When personal data is stored on any portable computer system, USB 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 once it has been transferred or its use is complete.

Use of Mobile Phones and Personal Devices

- Mobile phones and other devices will not be used for personal use during formal school time.
- Mobile phones will not be used during lesson time unless as part of an approved and directed curriculum-based activity with consent from a member of staff.
- Mobile phones and personally-owned devices should be switched off or on silent at all times in a secure place. (This includes staff, visitors and members of the school community)
- Mobile phones are forbidden on trips unless consent has been given by a member of staff.
- Staff to use school owned devices for the taking and collection of evidence which involve images or videos.
- No images or videos should be taken on any mobile phones or personally-owned mobile devices without the prior consent of the person or people concerned.
- Mobile phones and personally-owned mobile devices brought in to school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personally-owned mobile phones or mobile devices.
- Staff have the right to confiscate and search pupil's devices if a safeguarding incident has been brought to their attention. Any evidence will be taken and stored appropriately.
- The sending of abusive or inappropriate messages is forbidden.
- If a pupil breaches the school policy then the phone or device will be confiscated and will be held in a secure place in the school office and parents informed.
- If a pupil needs to contact his or her parents or carers, they will be allowed to use a school phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office.
- Pupils should protect their phone numbers by only giving them to trusted friends and family members. Pupils will be instructed in safe and appropriate use of mobile phones and personal devices and will be made aware of boundaries and consequences.

Pupil Mobile Phone Agreement (See Mobile Phone AUP)

- I know that mobile phones are not allowed to be used during the school day or around the school premises and are advised to be left at home.
- If consent has been given to me by my teacher then my mobile phone will be switched off / silent and kept in my school bag at all times during the school day.
- If I need to contact my parents/carers during school time, I will to go to the school office where the office staff will phone on my behalf.
- Permission by the teacher will be given to me if I can use a mobile phone in or around school or take it on a school visit.
- I know not to use text, voice messages, take images or use any internet connection to bully, upset or shock anyone in and out of school.
- I know that no images or videos should be taken on any mobile phone or personally-owned mobile devices in school without the consent of the person or people it involves.
- I know that the school is not responsible for any loss or damage to my mobile phone or any device I bring onto the school site.
- I understand that the school have a right to confiscate, search and keep any evidence on any mobile devices I bring into school.
- I know that I should protect my phone number by only giving them to trusted friends and family.

SMART Rules to be on display

Resources and Organisation

RESOURCES

ThinkUKnow - http://www.thinkuknow.co.uk/

Childnet International - http://www.childnet-int.org/

Kidsmart: http://www.kidsmart.org.uk/default.aspx

Know It All - http://www.childnet-int.org/kia/

Cybersmart - http://www.cybersmartcurriculum.org/home/

Chatdanger - http://www.chatdanger.com/

Digizen – cyber-bullying films: http://www.digizen.org/cyberbullying/film.aspx

NCH - http://www.stoptextbully.com/

ADVICE FOR PROTECTING CHILDREN

Child Exploitation and Online Protection Centre (CEOP) - http://www.ceop.gov.uk/

The Byron Review ("Safer Children in a Digital World") http://www.dcsf.gov.uk/byronreview/

CYBER BULLYING

http://www.teachernet.gov.uk/wholeschool/behaviour/tacklingbullying/cyberbullying/

http://www.teachers.gov.uk/wholeschool/behaviour/tacklingbullying/safetolearn/

Cyberbullying.org - http://www.cyberbullying.org/

SOCIAL NETWORKING

Digizen – "Social Networking Services" - http://www.digizen.org.uk/socialnetworking/

DATA PROTECTION

Information Commissioners Office - Data Protection:
http://www.ico.gov.uk/Home/what_we_cover/data_protection.aspx