E Safety and Social Media Policy

Rationale

New technologies are integral to the lives of children and young people in today's society.. The internet and other digital and information technologies are powerful tools which open up new opportunities for everyone. Electronic communication helps teachers, students and parents learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe internet access at all times. However, new technologies can put young people and the adults who work with them at risk within and outside of school, and it is with a view to safeguarding that this policy is created.

Aims

- To provide a framework for students and staff to recognise and avoid risk, and for remaining safe when using new technologies and the internet
- To demonstrate our commitment to safeguarding our school community

Guidelines

- A planned and up-to-date e safety programme will be provided as part of computing and Life curriculums, covering both the use of ICT and new technologies inside and outside of school
- Acceptable use agreements will be signed by students and parents/ carers yearly and a display on log-in screens will remind users of their responsibilities
- Staff acceptable use agreements will be signed on receipt of their staff laptops
- The school journal will contain simple messages about safe use of the internet and protecting passwords
- Key e-safety messages will be reinforced in assemblies and through curriculum content
- Students will be taught explicitly to be critically aware of the materials/ content they access on-line and be guided to validate the accuracy on information from three independent sources
- Students will be taught to acknowledge the source of information and to respect copyright
- In lessons where internet use is pre-planned, students will be guided to sites checked for suitability by staff and the Network manager will be informed if any unsuitable materials are found. Impero or close monitoring by staff will occur when "free" searches of the internet are suggested. Impero can be used to allow only specific sites and can block internet use completely

Responsibilities have been identified for different members of the school community and as such these will be at different levels depending on the position of the individual or group within the school. Our core responsibilities to e-safety are:

Governing Body

- Approving the E safety policy and reviewing its effective implementation
- Ensuring that the school complies with safeguarding legislation, particularly in response to e-safety and social media
- Receiving a yearly report on bullying incidents to include details of e safety issues

Head teacher and Senior Leaders

- Ensuring the safety of staff and students
- Ensuring that the E safety policy, and its related procedures and strategies, are implemented, monitored and reviewed
- Ensuring that the Senior Team link for ICT will be the E Safety co-ordinator for the school alongside the designated teacher for Child Protection but may delegate reporting, intervention or monitoring day-to-day to other ST members
- Ensuring that ***all*** staff are aware of their responsibilities
- Taking appropriate action against staff or students who breach the guidelines
- Ensuring that students, parents, staff and governors are regularly updated on e-safety guidance and messages, including in training of new staff, delivering assemblies or providing guidance during parents' evenings or through parent portal
- Collecting information on the numbers of incidents and reporting to Governors annual

Designated Child Protection lead

- Ensuring that child protection procedures are followed up appropriately in regard to e safety breaches or reports
- Contacting the police when incidents of "trolling" or bullying/ harassment occur, particularly those that occur outside of school hours

Network Manager/ technical staff

- To ensure that the school's ICT infrastructure is secure and not open to misuse or malicious attack
- To ensure the school meets external technical requirements outlined in LA guidance, South West Grid for Learning Security Policy guidance and Acceptable use Policies
- Provide users access to the school's network through properly enforces password protection policy in which passwords are regularly changed
- Ensuring that the school's filtering policy is applied and updated on a regular basis, and that its implementation is not the sole responsibility of any one single person (Appendix 4)
- To regularly monitor OSCAR/ network/ remote access in order to identify misuse or attempted misuse. This should then be reported to the E safety co-ordinator
- To provide technical support to those investigating any breaches of acceptable use
- Monitoring software systems, such as Impero, are implemented and updated as appropriate
- To review classroom IT activity and report breaches

All staff, to include supply staff and ITT students

- Responsible for using the school's ICT system in accordance with the Staff Acceptable Use agreement (Appendix 2)
- To engage in appropriate training activities to update knowledge
- To read, sign and abide by acceptable use agreements
- To challenge and log all incidents of e-safety or acceptable use breaches on SIMS and send a message (via SIMS or email) to alert there is a safeguarding matter (House Co-ordinator/Head of House or DYS/HBE/TBL)
- To promote safe use of mobile devices and the internet
- To keep their password secure and close down/ lock laptops when not in use
- To ensure that they will not invite, accept or engage in communications with parents or students within the school community in any personal social media
- To report any communication received from students on any personal social media sites to the E safety co-ordinator
- To report any inappropriate communications involving students or staff in any social media to either Child Protection leads or the Headteacher
- To ensure their own privacy by using the highest privacy settings levels on all personal social media accounts
- To use email communications to parents, staff or students from official school accounts in an appropriate or acceptable manner
- To consider the reputation of the school in any posts or comments related to the school on any social media or on the internet
- To refuse requests from any current students or past students who are under eighteen as a friend, follower or subscriber or similar on any personal social media accounts
- To inform students about the risks associated with taking, sharing, publication and distribution of images
- To recognise the risks associated with sharing their own images via the internet or on social media
- To use digital imagery/ video to support educational aims whilst following school guidelines in terms of consent of parents/ carers
- To teach explicitly critically awareness of the materials/ content that students access on-line and guide them to validate the accuracy of information from three independent sources
- To teach students to acknowledge the source of information and to respect copyright
- To guide students (in lessons where internet use is pre-planned) to sites checked for suitability and to inform the Network manager if any unsuitable materials are found
- To use Impero or closely monitor students when "free" searches of the internet are suggested. Impero can be used to allow only specific sites and can block internet use completely

- Students' work can only be published on-line with their permission and that of their parents

Students

- Responsible for using the school ICT systems in accordance with the Student Acceptable Use Agreement (Appendix 3). This will be signed during tutor time and no access to the school system will be given without this consent
- To take care when sharing images on-line. Students must never use, share, publish or distribute images of others with their express permission
- To provide feedback to the school in support of developing E-safety strategies

Parents/ Carers

- To support their children to adhere to the Student Acceptable Use agreement both within and outside of school
- Support school based sanctions when agreements are broken
- To provide feedback to the school in support of developing E-safety strategies
- To sign parental agreement for child's acceptable use on entry to the school

Community Users/ Visitors

- To agree to the Acceptable Use policy before being given access to the school systems

Additional issues

Training of staff and governors

- Routine training will be given to staff and governors to ensure they understand their responsibilities as outlined within the policy in line with Child Protection. All new staff will be trained during their ICT induction session

Technical- infrastructure/ equipment, filtering and monitoring

- The school will be responsible for ensuring that the school infrastructure is secured against physical attacks, accidental damage, and malicious software as is reasonably possible. Use of a firewall, antivirus software, physical restriction/ filtering system is mandatory. There will be regular reviews and audits of safety and security of school systems
- All users will be provided with a user name and password by the Network Manager who will keep up-to-date records of usernames, access rights and group memberships which will be reviewed at least annually. Staff will be required to change their passwords every month
- The master administrator passwords will be used by the Network Manager but also must be available to the Business Manager, Headteacher or nominated Senior team member
- Filtering will be maintained by the Network Manager and any requests to switch off the filtering/ unblock sites will go through the following process. Short term (for example, 1 period/ 1 day) requests to HOF who will make the IT support request. Longer term requests(for example, unblocking of sites permanently) to be reviewed by the ICT Strategy group.
- ICT staff will regularly monitor and record activity of users on the school network
- Temporary access for "guests" will be agreed via the IT Support request and the ICT Strategy group

Recording Incidents

All incidents should be recorded on the central Information Management System.
For incidents that involve bullying behaviours, specific coding is required on this system to recognise the roles of participants.
Additionally, bullying reporting will occur via the Sentinel system to the Local Authority.

Breaches of the Policy

Breaches will be thoroughly investigated and school based sanctions will apply, see Appendix 1.

Conclusion

The successful implementation of this policy will ensure that all members of the school community feel safe and secure (both physically and digitally) whilst at school. The school's values will live within the establishment and the every child matters agenda will be fulfilled.

Committee: Student Support & Progress Other related Policies

Approved: Jan 2016
Review Date: Jan 2018

Anti Bullying Policy
Bullying and Harassment for staff
Behaviour policy
Child Protection Policy
Inclusion Policy

Appendix 1: Grid for responses to misuse

A record of incidents will be held in the Student Support area ICT Misuse sanctions

	1st incident	2nd
L1 · **Allowing other people to know your password** · **Allowing other people to use your account**	Conversation with MoS	Blocked from using system for 1 week
L2 · **Playing games during lessons** · **Surfing the internet without permission** · **Accessing inappropriate material on the internet, including using proxy servers to avoid school filtering systems**	Faculty detention	Blocked from using system for 1 week Head's detention
L3 · **Taking ICT equipment apart** · **Viewing pornographic or offensive material.** · **Minor damage to systems** · **Doing unauthorised administrative tasks**	Blocked from using system for 1 week Head's detention Recorded as a Child Protection incident, if appropriate	Blocked for longer period at discretion of AHT PCSO involved(where pornography/offensive materials) and recorded as a Child Protection incident Liable for cost of damage
L4 · **Unauthorised installation of software** · **Making system software unusable** · **Deliberate hacking / wilful damage** · **Distribution of pornographic materials**	Blocked for longer period at discretion of AHT PCSO involved(where pornography/hacking) recorded as a Child Protection incident	Blocked from system at discretion of AHT Police involved and recorded as a Child Protection issue Liable for cost of damage

Appendix 2: Acceptable use policy for staff

This Acceptable Use Policy is intended to ensure that:

- Staff will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- School ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- Staff are protected from potential risk in their use of ICT in their everyday work.

The school will try to ensure that staff will have good access to ICT to enhance their work, to enhance learning opportunities for students learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that students receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed e-safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications and I understand that the school system is to be used for professional purposes only.
- I understand that the rules set out in this agreement also apply to use of school ICT systems (e.g. school provided laptops, webmail, OSCAR, etc) out of school.

- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using school ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (eg on the school website / VLE) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only communicate with students and parents / carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.
- I will lock my computer whenever it is unattended.
- I will not show students, or make it possible for students to access, SIMS, email or any other system that contains confidential information.
- I will not engage with students, parents/carers on social networking sites other than for educational purposes.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my personal mobile/ external devices (PDAs / laptops / mobile phones / USB devices / iPads / iPhones etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use.
- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programs or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads (including email attachments – max size 30MB) that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on any machine (including school provided laptops), or store programmes on a computer, nor will I try to alter computer settings, unless I have permission to do so from the IT Support.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the South Gloucestershire Council Data Protection Leaflet
- I understand that the data protection policy requires that any staff or student data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will not store any sensitive or confidential information on any of my own devices (including memory sticks, personal email accounts, etc) and any data stored on a school machine leaving site will be encrypted securely.
- I will immediately report to the IT Support any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

- I will not download any material from any illegal source (e.g. bit torrent, file sharing/P2P sites), or store such on a school owned machine.

I understand that I am responsible for my actions in and out of school:
- I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment out of school and my use of personal equipment in school or in situations related to my employment by the school.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action.

I have read and understand the above and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Signed: **Date:**

Appendix 3: Acceptable use policy for students
Students are responsible for good behaviour on the school network, email and the internet, just as they are in a classroom or a school corridor. General school rules therefore apply.
The following are not permitted:
- Using proxy servers to avoid school filtering systems
- The deliberate sending or displaying of offensive messages or pictures
- Using obscene language, harassing, insulting or attacking others. This kind of behaviour will always be reported to the police
- Sending of files/ attachments to emails which are not decent
- Transmitting of materials which are offensive or not connected with school
- Violating copyright laws
- Using others' passwords
- Using chat lines, chat applications, message sending, Twitter or Facebook will only be possible when sanctioned specifically by a member of staff
- Trespassing in others' folders. Work or files including system "out of bounds areas"
- Intentionally wasting resources (only download, save or print items which are for classwork, project or coursework/ controlled assessment purposes)
- Disks/Sticks/ Downloads containing programs must not be used on or loaded onto the school computers (data files, word processed text may be uploaded with permission)

As a user of the school network, the internet and email, I agree to comply with the school rules on their use. I will use the network, internet and email in a responsible way and observe all the restrictions detailed in the acceptable use policies.
Signed_____ Date_____

Appendix 4
South West Grid for Learning Filtering

- SWGfL Child Abuse Images List
- SWGfL .mp3 Download List
- SWGfL Web-Based Chat List
- SWGfL Web-Based Social Networking List
- SWGfL Non-Educational Games List
- SWGfL Pornography and Illegal or Age-Restricted Activity List
- SWGfL Violence List
- SWGfL Intolerance List
- SWGfL Drugs and Substance Abuse List
- SWGfL Proxy Bypass and Secure Search List

Social media guidelines

When using social media for educational purposes, the following practices will be observed:

- Staff should set up a distinct and dedicated social media site or account for educational purposes. This should be entirely separate from any personal social media accounts held by that member of staff and should ideally be linked to an official school email account. The form CSSSubject is preferred
- The URL and identity of the site should be agreed with the Head of Faculty before access is permitted to students
- The content of school social media sites should be solely professional and should reflect well on the school
- Staff must not publish photographs of students without reference to the written annual consent of parents/carers, or identify any students directly with full names or allow personal information to be published on these sites
- Care must be taken that any links to external sites from accounts are appropriate and safe
- Any inappropriate comments on or abuse of school-sanctioned social media should be reported immediately to the E safety co-ordinator or the CP leads
- Staff should not engage in any direct messages with students through social media where the message is not public
- Students can be friends, followers, subscribers on school sanctioned social media sites but staff will not follow students/ profiles

Mobile Technologies Use guidelines

If staff wish to use their own mobile or portable devices such as ipads, mobile phones within the school wireless system, they should contact IT support who will configuration access settings for the school network. If staff have visitors who require guest wireless access, staff should complete an IT Support request.

Currently, there is no capacity on the school wireless system for student's personal mobile devices therefore currently this is not possible. This will be kept under review.

Data Protection guidance

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