BANWELL PRIMARY SCHOOL

Online Safety Policy

Last Update:
October 2017

Approved:
FGB
November 2017

Next Update:
November 2018

To be reviewed annually

This policy sets out the ways in which the school will:
- **Educate and inform all members of the school community on their rights and responsibilities whilst using of technology**
- **build both an infrastructure and culture of online Safety**
- **work to empower the school community to use the Internet as an essential tool for life-long learning.**
- **This policy is used in conjunction with other school policies.**

Rationale

This policy applies to all members of the school community (including staff, pupils, volunteers, parents/carers, visitors and community users) who have access to and are users of school ICT systems. The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents such as cyberbullying, which may take place out of school, but are linked to membership of the school. The school will manage Online-safety as described within this policy and associated behaviour and anti-bullying policies, and will inform parents and carers of known incidents of inappropriate Online-safety behaviour that take place in and out of school.

Schedule for Development, Monitoring and Review
- The Implementation of the Online-safety policy will be monitored by an Online-safety committee, (Clare Gibbs (online safety lead), Kelly Oxley-Reed (online safety governor), Claire Pocock, (head teacher), Ben Summers (computing lead) and Louise Henry, safeguarding lead governor.

The impact of the policy will be monitored by the Online-safety committee by looking at:
- Log of reported incidents
- Surveys or questionnaires of parents and carers
- Future developments

The Online-safety policy will be reviewed annually or more regularly in the light of significant new developments in the use of technologies, new threats to online safety or incidents that have taken place.

Should serious online incidents take place, the LA safeguarding officer, LA ICT manager and the police would be informed.

Overview of responsibilities

The **Headteacher** is responsible for ensuring the safety (including online) of all members of the school community, though the day to day responsibility for online can be delegated.

The **Online-safety Leader**, working with the designated **Child Protection Coordinator**, will have overview of any serious child protection issues to arise from sharing of personal data, access to illegal or inappropriate materials, inappropriate on-line contact with adults, potential or actual incidents of grooming and cyber bullying. They ensuring and monitor the teaching of online safety within the classrooms and respond to the needs of teachers.

An **Online-safety committee** will work with the Online-safety Leader to implement and monitor the Online-safety policy and AUPs (Acceptable User Policies). Pupils will also form part of this group, working with them through the school council and health and safety team, to contribute their knowledge and use of technology. They meet three times a year.

Role Responsibility

Governors
- Approve and review the effectiveness of the Online-safety Policy
- Delegate a governor to act as Online-safety link
- Online-safety Governor works with the Online-safety Leader to carry out regular monitoring and report to Governors

Headteacher and Senior Leaders
- Ensure that all staff receive suitable CPD to carry out their Online-safety roles
- Create a culture where staff and learners feel able to report incidents
- Ensure that there is a system in place for monitoring Online-safety
- Follow correct procedure in the event of a serious Online-safety allegation being made against a member of staff or pupil
- Inform the local authority about any serious Online-safety issues
- Ensure that the school infrastructure/network is as safe and secure as possible. Ensure that policies and procedures approved within this policy are implemented

Online-safety Leader
- Lead the Online-safety committee
- Log, manage and inform others of Online-safety incidents
- Lead the establishment and review of Online-safety policies and documents
- Ensure all staff are aware of the procedures outlined in policies relating to Online-safety
- Provide and/or broker training and advice for staff
- Attend updates and liaise with the LA Online-safety staff and technical staff
- Meet with Senior Leadership Team and Online-safety Governor to regularly discuss incidents and developments
- Coordinate work with the school's designated Child Protection officer.
- Use the Online Compass tool 360 safe to review Online-safety

Teaching and Support Staff
- Participate in any training and awareness raising sessions
- Read, understand and sign the Staff AUP
- Act in accordance with the AUP and Online-safety Policy
- Report any suspected misuse or problems to the Online-safety Leader
- Monitor ICT activity in lessons, extracurricular and extended school activities

Pupils
- Read, understand and sign the Pupil AUP and the agreed class internet rules
- Participate in Online-safety activities, follow the AUP and report any suspected misuse
- Understand that the Online-safety Policy covers actions out of school that are related to their membership of the school

Parents and Carers
- Have a copy of the Pupil AUP
- Discuss Online-safety issues with their child(ren) and monitor their home use of ICT systems (including mobile phones and games devices) and the internet
- Access the school website in accordance with the relevant school AUP
- Keep up to date with issues through newsletters and other opportunities
- Inform the Headteacher of any Online-safety issues that relate to the school

Technical Support Provider
- Ensure the school's ICT infrastructure is as secure as possible
- Maintain and inform the Online-safety Leader of issues relating to filtering
- Keep up to date with Online-safety technical information and update others as relevant
- Ensure use of the network is regularly monitored in order that any misuse can be reported to the Online-safety Leader for investigation
- Ensure monitoring systems are implemented and updated
- Ensure all security updates are applied (including anti-virus and Windows)

Community Users
- Sign and follow the Guest/Staff AUP before being provided with access to school systems

Education of pupils
A progressive planned Online-safety education programme takes place through discrete lessons and across the curriculum, for all children in all years, and is regularly revisited.
- Key Online-safety messages will be reinforced through assemblies and Safer Internet Day (February) and throughout all lessons.
- Pupils are taught to keep themselves safe online and to be responsible in their use of different technologies as detailed in the CEOP: Think you know and ELIM lesson plans and materials.
- Pupils are guided to use age appropriate search engines for research activities.
- Staffs are vigilant in monitoring the content of the websites visited and encourage pupils to use specific search terms to reduce the likelihood of coming across unsuitable material.
- In lessons where internet use is pre-planned, pupils are guided to sites checked as suitable for their use and processes are in place for dealing with any unsuitable material that is found in internet searches.
- Pupils are taught to be critically aware of the content they access on-line and are guided to validate the accuracy and reliability of information.
- Pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Pupils will contribute to and sign an AUP for their class at the beginning of each school year, which will be shared with parents and carers.

Education and information for parents and carers

Parents and carers will be informed about the ways the internet and technology is used in school. They have a critical role to play in supporting their children with managing Online-safety risks at home, reinforcing key messages about Online-safety and regulating their home experiences. The school supports parents and carers to do this by:

- Providing clear AUP guidance which they are asked to sign with their children
- Inviting parents to attend activities such as Online-safety meetings as appropriate.

Education of wider school community
The school provides information about Online-safety to organisations using the school website.

Training of Staff and Governors
There is a planned programme of Online-safety training for all staff and governors to ensure they understand their responsibilities, as outlined in this, and the AUPs. This includes:
- An annual audit of the Online-safety training needs of all staff.
- All new staff receiving Online-safety training as part of their induction programme.

- The Online-safety Leader receiving regular updates through attendance at SWGfL and LA training sessions and by reviewing regular Online-safety newsletters from the LA.
- This Online-safety Policy and its updates being shared and discussed in staff meetings.
- The Online-safety Leader providing guidance and training as required to individuals and seeking LA support on issues.
- Staff and governors are made aware of the UK Safer Internet Centre helpline 0844 381 4772 and website http://www.saferinternet.org.uk

Cyberbullying

Cyberbullying (along with all other forms of bullying) of any member of the school community will not be tolerated. Full details are set out in the school's policy on anti-bullying and behaviour.

- the school will follow procedures in place to support anyone in the school community affected by cyberbullying.
- all incidents of cyberbullying reported to the school will be recorded.
- the school will follow procedures to investigate incidents or allegations of cyberbullying.
- Pupils, staff and parents and carers will be advised to keep a record of the bullying as evidence.
- the school will take steps where possible and appropriate, to identify the bully. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police.

Pupils, staff and parents and carers will be required to work with the school to support the approach to cyberbullying and the school's Online-safety ethos.

Sanctions for those involved in cyberbullying will follow those for other bullying incidents and may include:

- The bully will be asked to remove any material deemed to be inappropriate or a service provider may be contacted to remove content if the bully refuses or is unable to delete content.
- Internet access may be suspended at the school for a period of time. Other sanctions for pupils and staff may also be used in accordance to the schools anti-bullying, behaviour policy or AUP.
- Parent and carers of pupils will be informed.
- The police will be contacted if a criminal offence is suspected.

Technical Infrastructure

The school ensures, when working with our technical support provider that the following guidelines are adhered to:

- The School ICT systems are managed in ways that ensure that the school meets Online-safety technical requirements
- There are regular reviews and audits of the safety and security of school ICT systems.

Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations etc from accidental or malicious attempts which might threaten the security of the school systems and data with regard to:

- the downloading of executable files by users
- the extent of personal use that users (staff/pupils/community users) and their family members are allowed on laptops and other portable devices used out of school
- the installing programs on school devices unless permission is given by the technical support provider or ICT leader
- the use of removable media (e.g. memory sticks) by users on school devices.
- the installation of up to date virus software

Access to the school network and internet will be controlled with regard to:

- users having clearly defined access rights to school ICT systems through group policies
- users (apart from Foundation Stage) being provided with a username and password

- users being made aware that they are responsible for the security of their username and password and must not allow other users to access the systems using their log on details
- users must immediately report any suspicion or evidence that there has been a breach of security
- an agreed process being in place for the provision of temporary access of "guests" (e.g. trainee teachers, visitors) onto the school system. All "guests" must sign the staff AUP and are made aware of this Online-safety policy
- Foundation stage and Key Stage 1 pupil's access to the internet will be by adult demonstration with directly supervised access to specific and approved online materials
- Key Stage 2 pupils will be supervised. Pupils will be encouraged to use age-appropriate search engines and online tools and activities which will be adult directed
  The internet feed will be controlled with regard to http://bit.ly/tech_esafety_check
- the school maintaining a managed filtering service provided by SWGfL
- the school monitoring internet use
- requests from staff for sites to be removed from the filtered list being approved by the Senior Leadership Team and logged
- requests for the allocation of extra rights to users to by-pass the school's proxy servers being recorded, agreed and logged
- any filtering issues being reported immediately to SWGfL

The ICT System of the school will be monitored with regard to:

- the school ICT technical support regularly monitoring and recording the activity of users on the school ICT systems
- Online-safety incidents being documented and reported immediately to the Online-safety Leader who will arrange for these to be dealt with immediately in accordance with the AUP

Data Protection
The SWGfL Data Protection Policy provides full details of the requirements that need to be met in relation to the Data Protection Act 1998.

Use of digital and video images
Photographs and video taken within school are used to support learning experiences across the curriculum and to provide information about the school on the website. In order to protect children who are at risk, the school will:
- When using digital images, instruct staff to educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images including on social networking sites.
- Allow staff to take images to support educational aims, but follow guidance in the acceptable use policy concerning the sharing, distribution and publication of those images.
- Make sure that images or videos that include pupils will be selected carefully and will not provide material that could be reused.
- Make sure that pupils' full names will not be used anywhere on the school website, particularly in association with photographs.
- Written permission from parents or carers will be obtained before images or videos of pupils are electronically published (this is obtained on contact information forms which are updated annually)
- Not publish pupils' work without their permission and the permission of their parents.
- Keep the written consent where pupils' images are used for publicity purposes, until the image is no longer in use
- Parents are not allowed to take photographs on school trips using their own devices.

Communication

A wide range of communications technologies have the potential to enhance learning. The school will: with respect to email

- Ensure that all school business will use the official school email service.
- Ensure that any digital communication between staff and pupils or parents and carers (email, website etc) is professional in tone and content.
- Make users aware that email communications may be monitored.
- Inform users what to do if they receive an email that makes them feel uncomfortable, is offensive, threatening or bullying in nature.
- Teach pupils about email safety issues through the scheme of work and implementation of the AUP. .
- Only publish official staff email addresses.

with respect to personal publishing

- Teach pupils via age appropriate sites that are suitable for educational purposes. They will be moderated by the school where possible.
- Advise all members of the school community not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.
- Register concerns regarding pupils' use of email, social networking, social media and personal publishing sites (in or out of school) and raise with their parents and carers, particularly when concerning pupils' underage use of sites.
- Discuss with staff the personal use of email, social networking, social media and personal publishing sites as part of staff induction (see social networking policy)
- Outline safe and professional behaviour.

Assessment of risk

Methods to identify, assess and minimise risks will be reviewed regularly. As technology advances the school will examine and adjust the Online-safety Policy. Part of this consideration will include a risk assessment:

- looking at the educational benefit of the technology
- considering whether the technology has access to inappropriate material.

However, due to the global and connected nature of internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. The school cannot accept liability for the material accessed, or any consequences resulting from internet use. All users need to be reminded that the use of computer systems, without permission or for inappropriate purposes, could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to Police. As a school, Banwell will do their upmost to ensure that this is upheld.

Reporting and Response to incidents

- All members of the school community will be informed about the procedure for reporting Online-safety concerns (such as breaches of filtering, cyberbullying, illegal content etc).
- The Online-safety Leader will record all reported incidents and actions taken in the School Online-safety incident log and in any other relevant areas e.g. Bullying or Child Protection log.
- The designated Child Protection officer will be informed of any Online-safety incidents involving child protection concerns, which will then be escalated in accordance with school procedures.
- The school will manage Online-safety incidents in accordance with the School Behaviour Policy where appropriate.
- The school will inform parents and carers of any incidents or concerns in accordance with school procedures.

- After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes required.
- If the school is unsure how to proceed with any incidents of concern, then the incident may be escalated to the Safeguarding for Schools Adviser, Local Authority Designated Officer (LADO) or Senior ICT Adviser.

The police will be informed where users visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:

- child sexual abuse images
- promotion or conduct of illegal acts, under the child protection, obscenity, computer misuse and fraud legislation
- adult material that potentially breaches the Obscene Publications Act in the UK criminally racist material

Sanctions and Disciplinary proceedings

Sanctions and disciplinary procedures will be taken where users visit internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:

- pornography, adult or mature content
- promotion of any kind of discrimination, racial or religious hatred
- personal gambling or betting
- personal use of auction sites
- any site engaging in or encouraging illegal activity
- threatening behaviour, including promotion of physical violence or mental harm
- any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute
- use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by SWGfL and the school
- uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions
- revealing or publicising confidential or proprietary information (e.g. financial or personal information, databases, computer or network access codes and passwords)
- creating or propagating computer viruses or other harmful files
- carrying out sustained or instantaneous high volume network traffic (downloading or uploading files) that causes network congestion and hinders others in their use of the internet

Sanctions for misuse: Pupils

- The school will follow procedures in accordance with the behaviour policy.

Sanctions/Actions for misuse: Staff

Disciplinary proceedings will be followed and adhered to.

Mobile phones

The use of mobile phones is prohibited within the school grounds.

Visitors: Visitors are required to hand mobile phones and/or camera devices in to the office on arrival.
Pupils: Pupils are required to hand mobile phones and/or camera devices in to the office on arrival. Pupils are not permitted to use mobile phones or devices within the school grounds.
Staff: Staff are required to lock mobile phones away in a lockable unit and are only permitted to use these devices within the staff room and the office in school hours.

Social media

Schools/academies and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school / academy or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

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

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

Risk assessment School staff should ensure that:

- No reference should be made in social media to students / pupils, parents / carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school /academy or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.