AMESBURY CE VC PRIMARY SCHOOL

ONLINE SAFETY POLICY

Adopted by Staff: November 2016

Review due: November 2017

Digital Technology provides significant educational benefits, creating many opportunities for effective teaching and learning practices. Secure and effective internet access for students should be seen as an entitlement on the basis of educational need and an essential resource for staff. Whilst there are huge benefits, as a school, we also recognise that we must ensure appropriate, effective and safe use by all. This policy is designed to ensure that:

- All users are protected from inappropriate material, bullying and harassment.
- Users have access to resources to support learning and teaching.
- Users should be given clear boundaries on responsible and professional use.

Non-compliance by a member of staff is a serious matter and could be considered a disciplinary matter.

1. Leadership and Management

1.1 Development of policy

The Headteacher (Personal Development) is responsible for leading the development of the Online Safety Policy through consultation with staff, students and governors. The policy should be considered in conjunction with other relevant policies such as the Child Protection Policy (including Prevent), Behaviour Policy, Anti-bullying Policy and the Responsible Use Agreements for staff, governors and volunteers, and for students. Due to the rapidly changing world of information technologies, changes to current practices may be made at any time to ensure the safety of all users. This online policy has been written by the school, building on the Wiltshire online template policy and government guidance. It has been agreed by the senior leadership team and approved by governors. It will be reviewed annually.

1.2 Authorised Access

- The school commissions Internet Service Provision (ISP) from Oakford Internet Services. The ISP provides monitoring reports which are regularly checked to identify any attempts to access illegal content. The school will notify the local police and Wiltshire Council in these instances.
- The school will keep a record of all staff and students who are granted Internet access. The record will be kept up-to-date; for instance if a student's access is withdrawn.

1.3 Filtering and Monitoring

Despite careful design, filtering systems cannot be completely effective due to the speed of change of web content. However, the following procedures are in place:

- A log of all staff with unfiltered access to the Internet will be kept and regularly reviewed.
- A designated member of staff will review the popular permitted and banned sites accessed by the school.
- The school will work in partnership with parents, the Department for Education and its ISP to ensure systems to protect students are reviewed and improved.
- If staff or students discover unsuitable sites, the URL (web address) and content must be reported to the Internet Service Provider via the ITHelpdesk.
- Website logs will be regularly sampled and monitored by the Headteacher and Network Manager and any concerns reported to the SLT.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- Different levels of filters are applied to KS1 and KS2.

- Any material that the school believes is illegal or may place an individual at risk must be referred to the appropriate authorities i.e. Headteacher, Local Authority Designated officer (LADO), Police, Internet Watch Foundation.

1.4 Risk Assessment

As the quantity and breadth of the information available through the Internet continues to grow it is not possible to guard against every undesirable situation.

- Some material available via the Internet is unsuitable for students. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of 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.
- Methods to identify, assess and minimise risks will be reviewed regularly.
- The Headteacher will ensure that the Online Safety Policy is implemented and compliance with the policy monitored.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.

2. Teaching and Learning

2.1 The Curriculum

The Internet is an essential resource to support teaching and learning. The statutory curriculum requires students to be responsible, competent, confident and creative users of information and communication technology. In delivering the curriculum, teachers need to plan to integrate the use of communications technology such as web-based resources, e-mail and mobile learning. Computer skills are vital to access life-long learning and employment; indeed they are now seen as an essential life-skill.

- Internet use is a part of the statutory curriculum and a necessary tool for staff and students.
- The purpose of Internet use in school is to raise educational standards, to promote student achievement, ensure wellbeing, to support the professional work of staff and to enhance the school's management information and business administration systems.
- Whilst Internet access is an entitlement, users will need to show a responsible and mature approach to its use or this privilege may be removed.
- The Internet is an essential part of everyday life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.
- Students use the Internet widely outside school and need to learn how to evaluate Internet information and to take care of their own safety and security.

2.2 Enhancing Teaching and Learning

Benefits of using the Internet in education include:

- Access to a variety of worldwide educational resources
- Inclusion in the National Education Network which connects all UK schools
- Educational and cultural exchanges between students worldwide
- Vocational, social and leisure use in libraries, clubs and at home
- Access to experts in many fields for students and staff

- Professional development for staff through access to national developments
- Educational materials and effective curriculum practice
- Collaboration across networks of schools, support services and professional associations
- Improved access to technical support including remote management of networks and automatic system updates
- Access to learning wherever and whenever convenient

2.3 Evaluating Content

Information received via the web, e-mail or text message requires good information-handling and digital literacy skills. In particular it may be difficult to determine origin and accuracy, as the contextual clues may be missing or difficult to read. Ideally inappropriate material would not be visible to students using the web but this is not easy to achieve and cannot be guaranteed. Students will be taught what to do if they experience material that they find distasteful, uncomfortable or threatening.

- Students will be taught to be critically aware of the materials they read and how to validate information before accepting its accuracy.
- Students will use age-appropriate tools to research Internet content.
- 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.
- If staff or students discover unsuitable site or content they consider to be inappropriate, the URL (address) and content should be reported to the ITHelpdesk.
- The school will ensure that the use of Internet derived materials by staff and by students complies with copyright law.
- Students will be taught to acknowledge the source of information used and to respect individuals and intellectual property when using Internet material in their own work.

3. Communication and Content

3.1 Website Content

With regard to the school's website, publication of any information online should always be considered from a personal and school security viewpoint. Sensitive information will be published in the school handbook or on a secure online area which requires authentication. Editorial guidance will be used to ensure the website reflects the school's requirements for accuracy and good presentation.

- The point of contact on the school website should be the school address, school e-mail and telephone number. Staff or students' personal information will not be published.
- Parents or carers will be offered the opportunity to 'opt out' of having their child's photographs published e.g. on the school's website. This 'opt out' check will be conducted annually.
- Students' full names will not be used anywhere on the website in association with photographs.
- The nature of all items uploaded will not include content that allows the students to be identified, either individually or through aggregated pieces of information.
- The Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.
- The website should comply with the school's guidelines for publications including respect for intellectual property rights, privacy policies and copyright.

3.2 Managing e-mail

E-mail is an essential means of communication for both staff and students. Directed e-mail use can bring significant educational benefits and interesting projects between schools. However, the use of e-mail requires appropriate safety measures.

- Students may only use approved e-mail accounts on the school system and should be used in an acceptable way.
- Pupils may only send and receive emails from Amesbury Primary email addresses. Any attempts to do otherwise will be “bounced back” to the administrator.
- Sending images without consent, explicit images, messages that cause distress and harassment to others or are considered significant breaches of school Responsible Use Agreement and will be dealt with accordingly.
- Students must immediately tell a responsible adult if they receive offensive or distressing e-mail.
- Staff and governors must use secure e-mail for all professional communications and wherever possible, this should be via an official school provided email account
- E-mail sent to an external organisation should be written carefully and where appropriate, authorised before sending, in the same way as a letter written on school headed paper.

3.3 On-line communications and social media.

Online communications, social networking and social media services may be filtered in school by their ISP but are likely to be accessible from home.

All staff are made aware of the potential risks of using social networking sites or personal publishing either professionally with students or personally. They are also made aware of the importance of considering the material they post, ensuring profiles are secured and how publishing unsuitable material may affect their professional status.

Students are encouraged to think about the ease of uploading personal information, the associated dangers and the difficulty of removing an inappropriate image or information once published. They are taught about the importance of how to communicate safely and respectfully online, keeping personal information private.

- Users will be taught about how to keep personal information safe when using online services. Examples would include real name, address, mobile or landline phone numbers, school attended, email addresses, full names of friends/family, specific interests and clubs etc.
- Users must not reveal personal details of themselves or others in online communication, including the tagging of photos or video, or to arrange to meet anyone.
- Staff wishing to use social media tools with students as part of the curriculum will risk assess the sites before use and check the sites terms and conditions to ensure the site is age appropriate. Staff will obtain documented consent from the Senior Leadership Team (SLT) before using social media tools in the classroom.
- Staff official blogs or wikis should be password protected and only operate with approval from the SLT.
- Personal publishing will be taught via age appropriate sites that are suitable for educational purposes. They will be moderated by the school where possible.
- Students will be advised on security and privacy online and will be encouraged to set passwords, deny access to unknown individuals and to block unwanted communications. Student will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private.

- No member of the school community should publish specific and detailed private thoughts about the school, especially those that may be considered threatening, hurtful or defamatory.
- Parents wishing to photograph or video at an event they should be made aware of the school's expectations and be required to comply with the school's Responsible Use Agreement as a condition of permission to photograph or record.
- Concerns regarding students' use of social networking, social media and personal publishing sites (in or out of school) will be raised with their parents/carers, particularly when concerning students' underage use of sites.
- Staff personal use of social networking, social media and personal publishing sites will be discussed as part of staff induction and safe and professional behaviour will be outlined in the school Responsible Use Policy (School Business Manager).
- In line with, 'Guidance for Safer Working Practice for Adults who Work with Children and Young People' it is not considered appropriate for staff to engage in personal online communications with children and young people, parents or carers. Express care is also to be taken regarding the use of social networking sites. Staff are not permitted to 'friend' or communicate with students on social networking sites.

3.4 Mobile Devices (Including Bring You Own Device-BYOD)

Mobile devices refer to any device that provides access to the internet or internal network for example, tablet, e-readers, mobile phone, iPad, iPod touch or digital cameras. They can be used to facilitate communication in a variety of ways with text, images, sound and internet accesses all common features. The use of mobile devices is subject to the following key principles:

- Mobile devices that are brought in to school remain the responsibility of the user. The school accepts no responsibility for the loss, theft or damage of such items.
- School staff authorised by the Headteacher may search students or their possessions, and confiscate any mobile device they believe is being used to contravene school policy, constitute a prohibited item, is considered harmful, or detrimental to school discipline. If it is suspected that the material contained on the mobile device relates to a criminal offence, the device will be handed over to the Police for investigation.
- Sending abusive or inappropriate messages or content is forbidden by any user within the school community.
- Mobile devices may only be used during lessons or formal school time as part of approved and directed curriculum based activity.
- Mobile devices are not permitted to be used in certain areas or situations within the school site e.g. changing rooms or toilets, situations of emotional distress etc.
- Where staff may need to contact children, young people and their families within or outside of the setting in a professional capacity, they should only do so via an approved school account (e.g. e-mail or phone). In exceptional circumstances there may be a need to use their own personal devices and account; this should be notified to a senior member of staff as soon as possible. Social media will only be used for generic educational purposes.
- Staff should be provided with school equipment for the taking photos or videos of students linked to an educational intention. In exceptional circumstances staff may need to use personal devices for such a purpose and when doing so, should ensure they comply with the school's Responsible Use Agreement.
- For the safeguarding of all involved, users are encouraged to connect mobile devices through the school wireless provision and service that allows the ability to filter any device that uses the school Internet connection, without having to configure the user's own device.
- The school will take steps to monitor responsible use in accordance with the Responsible Use Agreement.

- All ipads should be password protected and be stored safely.

3.5 Video Conferencing

Video conferencing (for example FaceTime and Skype) enables users to see and hear each other between different locations. This 'real time' interactive technology has many potential benefits in education and where possible should take place using the school's wireless system.

- Staff must refer to any Responsible Use Agreements prior to students taking part in video conferences.
- All video conferencing equipment in the classroom must be switched off when not in use and not set to auto answer.
- Students will ask permission from a teacher before making or answering a video conference call.
- Video conferencing will be supervised appropriately for the students' ages and abilities.

3.6 Emerging Technologies

Many emerging communications technologies offer the potential to develop new teaching and learning tools, including mobile communications, Internet access, collaboration and multimedia tools. A risk assessment should be completed on each new technology and assessed for effective and safe practice in classroom use. The safest approach is to deny access until a risk assessment has been completed and safety has been established. Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

3.7 Cyber Bullying

Cyber bullying can be defined as 'The use of Information Communication Technology, particularly mobile phones and the internet to deliberately hurt or upset someone' DCSF 2007. For most, using the internet and mobile devices is a positive and creative part of their everyday life. Unfortunately, technologies can also be used negatively. It is essential that young people, school staff, parents and carers understand how cyber bullying is different from other forms of bullying, how it can affect people and how to respond and combat misuse. Promoting a culture of confident users will support innovation and safety. Cyber bullying (along with all other forms of bullying) of or by any member of the school community will not be tolerated. Full details are set out in the school's Anti-bullying Policy, Behaviour Policy and Child Protection Policy.

3.8 Data Protection

The quantity and variety of data held on students, families and on staff is expanding quickly. While this data can be very useful in improving services, data could be mishandled, stolen or misused. The Data Protection Act 1998 gives individuals the right to know what information is held about them and provides a framework to ensure that personal information is handled properly. It promotes openness in the use of personal information.

All data from which people can be identified is protected. Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998. See the Data Protection Policy for further details.

4. <u>Information Security</u>

4.1 Encryption of data

Staff are responsible for ensuring that they encrypt any data that is determined to be personal or commercially sensitive in nature. This includes data held on desktop computers, laptops, tablets and memory sticks. Staff must not remove or copy sensitive school data unless the media is: encrypted, transported securely and stored in a secure location. Staff should use the share point facility on Office 365 or the remote access facility to access documents at home.

4.2 Transmission of data

Sensitive and personal data must not be transmitted in unsecured emails. Where it is necessary to transfer such data, this transfer must be made via secure websites e.g. SecureNet Plus. If this is not available, the information must be at the least password protected, and preferably encrypted, before sending via email. If this method of transmission is used, the password must be sent by other means and on no account in the same email. A record of the email should be kept to identify when and to whom the email was sent.

4.3 Remote access

Remote access to data for staff is facilitated. This information must not be stored on any personal devices.

5. Implementation

5.1 Policy in Practice: Students

Many students are very familiar with Internet use and the culture that surrounds it. As part of the school's e-safety teaching and awareness-raising, it is important to discuss the key features with students as appropriate for their age. Students may need to be reminded of the school rules at the point of Internet use.

- All users will be informed that network and Internet use will be monitored.
- Online safety teaching should be integral to the curriculum and raise the awareness and importance of safe and responsible internet use amongst students.
- Online safety teaching will be included in the Computing and PSHE programmes and will cover safe use at school and home.
- Online safety rules and/or copies of the Responsible Use Agreement will be in student planners and on display.
- Safe and responsible use of the Internet and technology will be reinforced across the curriculum and subject areas.
- KS2 users have individual log ins to access computers.

5.2 Policy in Practice: Staff

It is important that all staff feel confident to use new technologies in teaching and the school's Online Safety Policy will only be effective if all staff subscribe to its values and methods. Staff are given opportunities to discuss the issues and develop appropriate teaching strategies. If a member of staff is concerned about any aspect of their ICT or internet use either on or off site, they should discuss this with their SLT to avoid any possible misunderstanding.

- The Online Safety Policy and the Staff, Governor and Volunteer Responsible User Agreement Appendix 2) are part of the child protection and safeguarding induction for all new staff. All staff are required to adhere to the Responsible Use Agreement.
- Staff are made aware that Internet traffic is monitored and can be traced to the individual user. Discretion and professional conduct is essential.
- Up-to-date and appropriate staff training in safe and responsible Internet use, both professionally and personally, will be provided for all members of staff.

- All members of staff will be made aware that their online conduct out of school could have an impact on their role and reputation within school. Civil, legal or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

- All staff have signed a responsible users agreement and signed to say that they have read the online safety policy and received the online safety training.

5.3 Policy in Practice: Parents

Parents need to be aware of the potential dangers that are associated with online communications, social networking sites and mobile technologies and to ensure their children are not putting themselves at risk.

Schools may wish to refer parents to websites referred to in the references section of this document.

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

- Parents are required to sign the Student Responsible User Agreement as part of the admissions process.

- A partnership approach with parents is encouraged. Information about online safety and resources specifically directed at parents and carers are included on the school's website under Child Protection and E-safety. Newsletters are also regularly used to update parents on online safety issues.

- Internet issues will be handled sensitively to inform parents without undue alarm.

- Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be made available to parents.

5.4 Handling of complaints

Parents and teachers must know how and where to report incidents in line with the school complaints procedure and complaints of a child protection nature must be dealt with in accordance with the Local Safeguarding Children Board Child Protection procedures. Prompt action will be required if a complaint is made. The facts of the case will need to be established, for instance whether the Internet use was within or outside school. A minor transgression of the rules may be dealt with by the teacher as part of normal class discipline. Other situations could potentially be serious and a range of sanctions will be required, linked to the school's behaviour policy. All record of the incident should be kept, e.g. e-mails saved or printed, text messages saved etc.

- Responsibility for handling incidents will be delegated to a senior member of staff.

- Any complaint about staff misuse must be referred to the Headteacher.

- Students and parents will be informed of the complaints procedure.

- Parents and students will need to work in partnership with staff to resolve issues.

- There may be occasions when the police or children's social care must be contacted. Early contact could be made to establish the legal position and discuss strategies.