E-Safety Policy

Status	Non Statutory	**Date created**	July 2018
Any other statutory names for this policy (where applicable)		**Date first approved**	November 2018
Responsibility for this policy (job title)	Deputy Headteacher	**Date last reviewed**	
Governors' Committee with responsibility for its review	Teaching & Learning	**Frequency of review**	Every three years **however as a new policy and with the introduction of 1:1 in Sept '18, the policy should be reviewed for Sept '19**
Tick here if Bucks Policy attached in its entirety		**To be put on the school website?**	Yes
Approval necessary	Sub Committee		

Introduction

Aylesbury High School recognises that Information Technology (IT) and the Internet are excellent tools for learning, communication and collaboration. These are accessible within the school for enhancing the curriculum, to challenge students and to support creativity and independence. Using IT to interact socially and share ideas can benefit everyone in the school community. However, it is important that the use of IT and the internet is continually reviewed and monitored across the school and that it is the responsibility of students, staff and parents[1], to use it appropriately and practise good e-safety. It is important that all members of the school community are aware of the risks and dangers of using the internet and how they should conduct themselves online.

E-safety does not just cover the Internet and available resources but all different types of devices and platforms (e.g. Chromebooks, Smartphones, wearable technology and other electronic communication technologies). The school understands that some adults and young people will use these technologies irresponsibly which may result in harm to young people. Aylesbury High School has a duty of care towards any staff, students or members of the wider school community, to educate them on the risks and responsibilities of e-safety. It is important that there is a balance between controlling access to the Internet and technology and allowing freedom to explore and use these tools to their full potential. This policy governs all individuals who are given access to the school's IT systems. This includes staff, governors and students. However, sections of this policy may not be relevant to all.

Aims

This policy aims to be an aid in regulating IT activity in school and provide a good understanding of appropriate IT use that members of the school community can use as a reference for their conduct online outside of school hours. E-safety is a whole-school issue and responsibility. Cyber-bullying by students will be treated as seriously as any other type of bullying and will be managed through the school's behaviour and exclusions procedures.

If there is a suggestion that a student is at risk of abuse or significant harm, the matter will be dealt with under the school's child protection and safeguarding procedures.

[1] Any reference to parent(s) implies parent(s) or carers(s)

Roles and responsibility

The Headteacher, Leadership Team and Governors will ensure that the E-safety Policy is implemented and adhered to and that compliance with the policy is monitored. The Learning for Life (L4L) Coordinator will undertake an annual review of how students may be taught about safeguarding, including online safety, through the school's PSHE provision, ensuring relevance, breadth and progression.

Communicating school policy

Staff guidance relating to their IT conduct is available in both the AHS Staff Code of Conduct and the Staff Handbook. Staff will also be reminded of E-Safety related guidance via the Weekly Bulletin and through training organised by the School, at appropriate times. Ditto, the online magazine is linked to the Weekly Bulletin for staff to read. E-safety is integrated into the curriculum in any circumstance where the internet or information technology is being used, as well as being specifically addressed in the L4L curriculum. At the start of each academic year, students will complete a Google form confirming that they agree to the AHS Acceptable Use Policy (see Appendix links at the end of this document) which is linked to the student homepage. Students complete this once they have been given their AHS school email address. Staff are also required to agree to the Staff Acceptable Use Policy using a similar Google form. The information gained from this process is monitored and reviewed by a member of the Leadership Team.

In common with other media such as magazines, books and video, some age or content specific 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 interlinked nature of internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer or device connected to the school network. The school makes every effort to ensure that students are unable to access inappropriate material via a Smoothwall filtering and monitoring system, however we cannot accept liability for the material accessed via non Aylesbury High School logins. Students are encouraged to raise any concerns through a Google form on the student homepage called ‘Report a Concern’. This form will be monitored by the Leadership Team.

If a student or member of staff requests access to a site that Smoothwall is blocking, the IT team will check a regularly updated document from Buckinghamshire County Council which lists sites that need to be blocked. The IT team also complete their own testing to ensure the site is safe; if the site links to social media or incorporates adverts access is not given.

Learning to evaluate internet content

With so much information available online, it is important that students learn how to evaluate internet content for accuracy and intent. This is approached by the school as part of digital literacy across all subjects in the curriculum. Students will be taught:

- To be critically aware of materials they read and shown how to validate information before accepting it as accurate, e.g. ‘fake news’.
- To acknowledge the source of information used and to respect copyright. The school will take any intentional acts of plagiary very seriously.
- About the risks associated with using the internet and how to protect themselves and their peers from potential risks.
- How to recognise suspicious, bullying or extremist behaviour.
- The definition of cyberbullying, its effects on the victim and how to treat each other's online identities with respect.
- The consequences of negative online behaviour.

- How to report cyberbullying and/or incidents that make students feel uncomfortable or under threat and how the school will deal with those who behave badly.

The school provides e-safety guidance to staff to better protect students and themselves from online risks and to deal appropriately with e-safety incidents when they occur. Ongoing staff development includes training on online safety together with specific safeguarding issues including cyberbullying and radicalisation.

Managing Information Systems

The school is responsible for reviewing and managing the security of the IT services and networks that it operates and takes the protection of school data and personal protection of the school community seriously. This means protecting the school network, as far as is practicably possible, against viruses, hackers and other external security threats. The security of the school information systems and users will be reviewed regularly by the IT Support Team and other third parties engaged with the school. A firewall called Smoothwall, monitors, filters and protects the network and connection to the internet. Smoothwall produces a report for the Head and Deputy Headteacher to view on a daily basis to highlight any inappropriate material students or staff have tried to access. Our Anti-Virus and Malware protection software is cloud based and provides a daily update which is monitored by the IT team. This system maintains a rolling 7 days of historical data~~.~~

Emails

The school uses email internally for staff and students and externally for contacting parents and conducting day to day school business and is an essential part of school communication.

The school has the right to monitor emails, attachments and their contents but will only do so if there is suspicion of inappropriate use.

Staff and students should regularly change passwords and ensure that passwords are effective, for example using 3 separate unconnected words.

School email accounts and appropriate use

Staff should be aware of the following when using email in school:

- Staff should use their school email accounts for school-related matters, contact with other professionals for work purposes and to communicate with students, parents or carers. Personal email accounts should not be used to contact any of these people.
- For any awkward, sensitive, easily misinterpreted situations or anything that may have legal repercussions, staff should have the content of their email checked carefully by a member of the Leadership Team.
- Staff must tell a member of the Leadership Team if they receive any offensive, threatening or unsuitable emails either from within the school or from an external account. They should not attempt to deal with this themselves.
- Staff should refer to the Data Protection and Confidentiality Policy before sending any sensitive or personal data via email.

All students receive a guide to IT use at the start of the academic year prepared by their form tutors in addition to compulsory computing lessons in KS3. Additional guidance is promoted through our L4L programme.

Students should be aware of the following when using email in school:

- Students will be taught to follow these guidelines through the IT and the L4L curriculum and in any instance where email is being used within the curriculum or in class.
- All students are provided with a school gmail account and students may only use approved email accounts on the school system during school hours.
- If a student contacts a member of staff using a non-school gmail account, the member of staff should reply to say 'that they need to resend the email using the appropriate account' and copy in their line manager. Staff should not respond to any further emails from the original email account unless the nature of the communication raises safeguarding concerns.
- Students are warned, via the Acceptable Use Policy and in L4L lessons not to reveal personal details of themselves or others in email communication or arrange to meet anyone without specific permission.
- Students should immediately inform a member of staff if they receive any offensive, threatening or unsuitable emails either from within the school or from an external account. They should not attempt to deal with this themselves.

Published content and the school website

The school website is viewed as a useful tool for communicating the school ethos and practice to the wider community. It is also a valuable resource for prospective parents and students, current parents, students and staff for keeping up-to-date with school news and events, celebrating whole-school achievements, personal achievements and promoting the school.

The website is in the public domain and can be viewed by anybody online. Any information published on the website will be carefully considered, by the Leadership Team, in terms of safety for the school community, copyrights and transparency policies.

The website will comply with the school's guidelines for publications including respect for intellectual property rights and copyright. Staff and students will be made aware of copyright in respect of material taken from the internet.

Policy and guidance for safe use of student's photographs and work

Colour photographs and students' work bring the school to life, showcase students' talents, and add interest to publications both online and in print that represent the school. However, the school acknowledges the importance of having safety precautions in place to prevent the misuse of such material.

Using photographs of individual students

Children or young people may not be approached or photographed while in school or doing school activities without the school's permission, except for parents taking photographs or videos at school events involving their child for personal use only.

The school follows general rules on the use of photographs and videos of individual students:

- Consent will be obtained from students or their parent (via the photograph opt out system) before using images in a way which is privacy intrusive. This may include images in a school publication, on the school website or videos made by the school or in class.
- Electronic and paper images will be stored securely.
- Staff are required to move any images taken as part of a school trip or activity from a device to a secure folder on the school system. They must ensure the images are removed from the device.

- Images will be carefully chosen by the member of staff using the images for publication to ensure that they do not pose a risk of misuse.
- For public documents, including in newspapers, full names will not be published alongside images of the student without the consent of the parent or the student (as appropriate). Groups may be referred to collectively by year group or form name.
- Events recorded by family members of the students such as House Drama or sports events must be for personal use only.
- Students are encouraged to tell a member of staff if they are concerned or uncomfortable with any photographs that are taken of them or they are being asked to participate in.
- Any photographers that are commissioned by the school will be fully briefed on appropriateness in terms of content and behaviour, will wear identification always, and will not have unsupervised access to the students.

Complaints regarding misuse of photographs or video

Parents should follow the school complaints procedure if they have a concern or complaint regarding the misuse of school photographs.

Social networking, social media and personal publishing

Personal publishing tools include blogs, wikis, social networking sites, chat rooms and instant messaging programmes. These online forums are the more obvious sources of inappropriate and harmful behaviour and where students are most vulnerable to being contacted by a 'dangerous' person. It is important that the school educates students so that they can make their own informed decisions and take responsibility for their conduct online. The school will block/filter access to social networking sites via the school network.

The school encourages parents with children under the age of 13 to follow the guidance of social media sites such as Facebook, Snapchat etc. and not give their child access.

Social media sites have many benefits, however both staff and students should be aware of how they present themselves online. Students are taught through the IT curriculum and L4L about the risks and responsibility of uploading personal information, including images, and the difficulty of removing the information completely once it has been made available in such a public place, often referred to as a 'digital footprint'. The school follows general rules on the use of social media and social networking sites in school:

- Students are educated on the dangers of social networking sites and how to use them in safe and productive ways. Students are advised never to give out personal details of any kind which may identify them or their location.
- Any sites that are to be used in class will be risk-assessed by the teacher in charge prior to the lesson to ensure that the site is age-appropriate and safe for use.
- Official school blogs created by staff or students as part of the school curriculum will be moderated by a member of staff and must be registered only against a school controlled email account.
- Students and staff are encouraged not to publish specific and detailed private thoughts, especially those that might be considered hurtful, harmful or defamatory. The school expects all staff and students to remember that they are always representing the school and must act appropriately.
- Safe and professional behaviour of staff online will be discussed at staff induction and guidance is provided through the Staff Code of Conduct and Staff Handbook.

Mobile phones and personal mobile electronic devices (Smartphones), including wearable technology

Mobile phones and other personal devices are now an important part of everyone’s life and have considerable value, particularly in relation to individual safety. Whilst these devices are commonplace today, their use and the responsibility for using them should not be taken lightly. Some issues surrounding the possession of these devices are that:

- they can make students and staff more vulnerable to cyberbullying
- they can be used to access inappropriate internet material
- they can be a distraction in the classroom
- they are valuable items that could be stolen, damaged or lost
- they can have integrated cameras, which can lead to child protection, bullying and data protection issues

The school’s expectation is that mobile devices will be used responsibly, at times agreed by the school. These expectations may vary from time to time but any changes will be clearly communicated to the school via daily notices on the student homepage or via form tutors.

Cyberbullying

Cyberbullying, as with any other form of bullying, is taken very seriously by the school. The anonymity that can come with using the internet can sometimes make people feel safe to say and do hurtful things that they otherwise would not do in person. It is made very clear to all members of the school community what is expected of them in terms of respecting their peers, members of the public and staff and any intentional breach of this will result in disciplinary action.

Any incidents of cyberbullying will be dealt with in accordance with the Behaviour and Exclusions Policy and, where appropriate, the school's Child Protection and Safeguarding Policy.

Managing emerging technologies

Technology is progressing rapidly and innovative technologies are emerging all the time. **Dataspire** and our on-site IT team will risk-assess any new technologies and proposed software before they are purchased or allowed in school.

Appendix

Acceptable Use Policy for Chromebook Users (Y7-10)

Acceptable Use Policy for BYOD