Alderbrook School | Alderbrook Sixth Form

E-Safety Policy

Author	K Fisher
Date	June 2018
Version	5
Approved Date	12.7.18
Review Date	June 2020

Responsibility for the E-Safety

1   The e-Safety Policy provides an important part of schools' safeguarding provision for students. E-safety is a whole school responsibility and a designated member of the senior management team has the overall responsibility for reviewing the policy. This policy will be reviewed as situations arise or as identified on the cover of the policy, whichever comes first, to keep it up to date and respond to the school's needs.

2   Alderbrook will take all reasonable precautions to ensure e-safety. However, owing to the international availability of internet content, the existence of mobile technologies and the speed of change, it is not possible to guarantee that there will never be unsuitable material on a school computer or mobile device. The school cannot accept liability for material accessed, or any consequences of internet access or ICT usage. Please also refer to the school's child protection policy since the aims of the child protection policy form the foundations of the e-safety policy.

3   The Governors will ensure the e-safety policy is implemented, monitored and reviewed. The Leadership (DHT and Head of ICT) have a duty of care to all students and will ensure that staff are aware of their responsibilities under the policy and are given appropriate training and support to fulfil their responsibilities. The Head of ICT will ensure that issues of e-safety and cyber bullying are addressed within the curriculum. The DHT will provide support for this through pastoral systems across the school.

4   The Network Manager and ICT Support Team will ensure the technical infrastructure is secure and not open to abuse. They will ensure the school's IT e-safety meets the requirements of Government, Local Authority and School e-safety policies. This will include ensuring that a robust password policy is enforced, that access rights are in place for all classes of user and that filtering and monitoring procedures are fit for the purpose of the policies.

5   All Staff will be aware of and adhere to the e-safety policy, reporting any concerns to IT support, Head of ICT or safeguarding personnel as appropriate.

6   Students should read and regularly accept the conditions of use on school PCs and report cyber bullying, abuse, misuse, and access to inappropriate materials directly to the teacher.

7   Parents should support the school in e-safety matters.

8   Visitors need to be aware of and agree to the acceptable usage policy (AUP) and accept access restrictions whilst on site.

The importance of the internet and appropriate uses

9   The rapid developments in electronic communications are having profound effects on society. Every student is younger than the World Wide Web and many use it more than their teachers. At Alderbrook, the internet is valued by both students and staff as a source of information and means of communication. It will be used appropriately in pursuance of acceptable school activities by both students and staff.

10   It is the responsibility of staff who use ICT in their lessons to effectively monitor and ensure appropriate use. Expectations of appropriate use are made clear to students in discreet ICT lessons and therefore students should be familiar with these expectations which need to be reinforced by all staff. RM tutor and other similar monitoring software are effective tools to

limit student access to websites which the class teacher feels are most useful for the learning activities of the lesson.

Using the internet for learning and planning

11   Alderbrook has invested significantly in computer hardware and improved Internet access so that learning needs can be addressed. We will continue to develop effective practice in Internet use for teaching and learning. Teachers will help students to learn how to select from the mass of information provided by the Internet by guiding them to appropriate websites, and teaching search skills. Students need to learn to evaluate everything they read and to refine their own publishing and communications with others via the Internet. In discreet ICT lessons, students are taught these essential skills across a range of units.

Students and E-safety

12   Many students are very familiar with Internet use and culture. Students' perceptions of the risks will vary; the rules for responsible use will need explanation and discussion. Once a week, or whenever content has been changed, students will need to accept the reasonable use policy when they log-on.

13   Cyber bullying will not be tolerated. Bullying can take a variety of forms, and may involve the use of text, images, graffiti, email, audio files, video messages, posting on web-sites or on various social media platforms. It can include making threatening, insulting or abusive comments, or sharing derogatory or embarrassing images or videos about someone online. The use of ICT to bully could be against the law. Abusive language or images used to bully, harass or threaten another, whether spoken or written (through electronic means) may be libellous and contravene the Harassment Act 1997 or the Telecommunications Act 1984. The nature and consequences of cyber bullying and how to support victims of cyber-bullying are addressed in Aspire / PSD lessons, in assemblies throughout the year and wherever else necessary in an age-appropriate and timely manner.

14   In ICT lessons, there are numerous opportunities to educate students on a range of e-safety issues - in particular a unit of work is dedicated to e-safety in year 7. Please see Appendix A for the content.

15   An assembly is delivered to all year groups once a year on the topic of E-Safety. This assembly highlights key ways students should use IT in a safe way in and outside of school and also reminds students on the school policy on using computers in an appropriate manner.

Material Focus

Staff use of ICT

16   It is important that all staff feel confident to use the Internet in teaching. Staff must read and understand the e-safety policy and act on the policy points. The Goverors and all staff including administration, site management and voluntary helpers should be included in appropriate awareness raising and training. The induction of new staff should cover Internet issues and appropriate uses of email communication. Below is a table of action staff should take together with examples of unacceptable use of ICT.

Required actions	Unacceptable use and misconduct
Monitor student activities which involve the use of ICT.	Publishing content on the internet (e.g. through personal Facebook accounts or other forums) which is inappropriate and compromises your status as a teacher
Report any cyber bullying to heads of college	Using personal e-mail addresses to communicate with students.
If cyber bullying takes place using school ICT equipment, report this to the e-safety coordinator who can take appropriate action	Taking photos or videos of students using mobile phones or any other personal digital recording or image capturing devices
If e-mailing students as part of learning activities, use a school email account and restrict the content of messages to the learning activity	Communicating with children using social networking sites
Check any media such as videos prior to using them in class to assess whether it is acceptable and appropriate. Seek advice if uncertain	Published photographs or videos of students without student or parent consent.
Lock school computers or laptops when away from them to avoid misuse by others and giving access to sensitive information	Allowing students access to material or data which is inappropriate for their use.

17   School e-mail should be used for school related business and not for personal communications. Formal email messages should be professionally formatted with an opening salutation and complementary signature. E-mails should be brief and to the point to avoid overloading colleagues with information. The content and tone of e-mail messages should be professional and non-threatening to avoid causing undue stress and anxiety to the recipient.

18   Misuse of internet facilities may constitute gross misconduct which can result in dismissal. If a member of staff is concerned about any aspect of their Internet use in school, they should discuss this with the headteacher or e-safety coordinator to avoid any possible misunderstanding. Information and guidance will be provided to staff in a clear and simple format.

Data Protection

19   In accordance with the general data protection regulations, staff are obliged to use, process and store data in line with the eight principles of the act included at the end of this sub-section. Specific regulation includes -

- In the workplace and out of the workplace, to log out of the school network when away from the computer system. The school network includes any medium which requires a

username and password including for example, the portal, e-mail and learning gateway. Alternatively, where there is an option to lock your computer system, use this facility providing you are the sole password holder.

- Student data or sensitive information must not be stored on removable media (USB flash or hard drives). Data must not be stored on network servers or transferred via your school Microsoft OneDrive account.
- Password protect any data files if removing them from the school network using a strong password (at least 8 characters, uppercase and lower case including special characters and numbers).
- Maintain a strong password for the school network logins in accordance with the above guidance.
- Handle data with due care and attention to prevent loss of data and to maintain accuracy.
- Do not share student data or sensitive information outside of the boundaries relating to its use, purpose and your role.
- Observe all policy points relating to the school's data protection policy.

20   The Seven Principles of the Data Protection Act 1998

- Lawfulness, fairness and transparency - Processing must meet the tests described in GDPR [article 5, clause 1(a)], What is processed must match up with how it has been described and Tell the subject what data processing will be done.
- Purpose limitation - Personal data can only be obtained for "specified, explicit and legitimate purposes"[article 5, clause 1(b)]. Data can only be used for a specific processing purpose that the subject has been made aware of and no other, without further consent.
- Data minimisation - Data collected on a subject should be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed".[article 5, clause 1(c)]
- Accuracy - Data must be "accurate and where necessary kept up to date" [article 5, clause 1(d)]
- Storage limitation - Personal data is kept in a form which permits identification of data subjects for no longer than necessary. [article 5, clause 1(e)] i.e. Data no longer required should be removed.
- Integrity and confidentiality (security) - Requires processors to handle data in a manner ensuring appropriate security of the personal data including protection against unlawful processing or accidental loss, destruction or damage. [article 5, clause 1(f)]
- Accountability – Data owners must be identifiable, Data subject rights and privacy must be built in by design.

Parents and E-safety

21   Parents should be aware of the dangers students may face with unrestricted access to the Internet and should ensure access to only age-appropriate use of social media and computer games in order to limit their child's exposure to online grooming, radicalisation, bad language, sex and violence. The school may be able to help parents plan appropriate supervised use of the Internet at home. However, parents are responsible for supervising their child's use of ICT outside of school.

22   The school will offer guidance and advice to parents about safe use of the internet to avoid cyber-bullying. Parents will receive a letter if their child has been involved in cyber-bullying (Appendix B) which will direct them to e-safety material on the school website including the Digital Parenting magazine. The school website also has a link to CEOP (Child Exploitation and Online Protection) for reporting any inappropriate or potentially illegal activity, online abuse or grooming with or towards a child to the police.

Managing published content

23   The school website will celebrate students' work, promote the school and publish resources for projects or homework. The website reflects the school's ethos and the school will endeavour to ensure that all information presented is accessible, well formatted, accurate and up to date.

24   The school website is publicly accessible. Information that might be considered private, privileged or involve security such as staff details or floor plans of the school premises should only be published in the school handbook or the intranet with access restricted as appropriate.

25   Published photographs should only identify named students when necessary – for example, prize winners or sporting achievements. Paintings, drawings or images of students' work or general photographs of an activity may often be more appropriate than individual photographs. Care must be taken when publishing photographs to ensure that all students are appropriately dressed and that no potential breaches of custom, convention or health and safety are depicted.

26   Photographs of a student should not be published without the parent's or carer's written permission. Similarly, photographs of school staff should not be published without express consent.

27   The school now has facilities such as Alderpedia which allow students to publish content including videos on the internet. Staff leading on these initiatives will review content for appropriateness before it goes live.

Filtering, Supervision and Monitoring

28   Levels of access and supervision must be appropriate for different sections of the school community and systems should be in place to adapt the access level according to staff / students' specific areas of study or needs. The internet filtering system will be managed by the ICT support staff in discussion with the senior management team.

e-filtering

29   The school uses a system for web filtering and monitoring. Certain categories of websites are blocked for all users such as pornography and gambling, or abusive and extremist sites. Additional websites may be blocked or allowed depending on user type and curriculum requirements at the time.

30   Staff and students are required to use the school provided email which is filtered for viruses, malware, offensive and distressing material by Solihull MBC. This is provided for everyone's protection and safeguarding.

31   The network infrastructure (wired and wireless) is protected from internet penetration by the SMBC firewall plus the onsite firewall. Wireless access is protected for domain devices and domain users. A guest SSID (wireless network) is provided to allow school visitors internet access only.

e-supervision

32   Classroom computer management is conducted through RM Tutor which provides real-time viewing of student screens, program white-list and black-list, Internet white- list and black-list.

e-monitoring

33   All student activity is monitored on the school PCs – this includes all website activity, emails, created and received files, typed entries and printing. The monitoring system will look for rude, offensive, racist, extremist or other material that might cause concern such as self-harm and bullying. User activity including username, date time and site visited is automatically monitored and logged by the servers. Archives of all activity are maintained for six months.

Appendix A

Lesson structure

Lesson 1: Social Media
Learning Objectives
- To know how to use privacy settings
- To be able to keep sensitive information about yourself hidden
- To recognise how users are accountable for the information or communication on social media websites.

Teaching and Learning Activities
- Class discussion about Students presence online and the importance of ensuring they use social media in a secure way
- Video: class discussion relating to using the internet. Students are given a series of questions to answer to test their understanding of what they need to do to ensure they are using social media in a secure way.

Homework
- Create a poster which which looks at their digital footpint.

Lesson 2: Cyberbulling
Learning Objectives
- Awareness of what cyberbullying is
  Identify ways to deal with cyberbullying

Teaching and Learning Activities
- Class discussion about What cyberbullying means
- Video: class discussion relating to the videos as displayed on the interactive whiteboard.
- Students answer questions to show their understanding of how to deal with cyberbulling
- Class discussion about cyber bullying and actions which can be taken

Homework
- Come up with a poster to advise students how to deal with cyberbullying

Lesson 3: Safe searching
Learning Objectives
- Gain skills in searching for information effectively and safely
- Awareness of information reliability and validity
- Knowledge of the different resources and assistance available for E-Safety

Teaching and Learning activities
- Class discussion about effective ways to search for information using the internet (key words and advance searches). Teacher demo (eg in searching for the planet Mercury the difference in result when entering 'Mercury' and being more specific with 'Planet Mercury'.
- Video: class discussion relating to the videos as displayed on the interactive whiteboard

- Students to work in small groups to search for information about the latest innovations relating to electric cars. Produce a single slide in Powerpoint about two facts they discovered, how they know it is a fact and how they carried out their search.
- Class discussion relating to information reliability on the internet.
- Recap key points relating to this programme of study and extra resources on the shared area (leaflets/brochures)

Homework
- Share the information about e-safety with your parents and a brother/sister