Alderbrook School | Alderbrook Sixth Form

E-Safety Policy

Author	K Fisher and J Howlett
Date	May 2024
Version	8
Approved Date	May 2024
Review Date	June 2026

Responsibility for E-Safety

1 The e-Safety Policy provides an important part of the 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 Trustees will ensure the e-safety policy is implemented, monitored and reviewed. The Leadership (Deputy Head Teacher (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, 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 The school will regularly communicate with parent/carers about e-safety and 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 a user of 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 At Alderbrook, Computing/ICT is regarded as a discreet subject which is used across the curriculum. It is the responsibility of staff who use Computing/ICT in their lessons to effectively monitor and ensure appropriate use. Expectations of appropriate use are made clear to students in Computing/ICT lessons and therefore students should be familiar with

these expectations which need to be reinforced by all staff. Smoothwall, NetSupport School and other monitoring tools are available 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 Computing/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. Students should read and understand the Students Acceptable Use Policy (Appendix B).

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 Computing/ICT lessons / Aspire / PSD lessons, in assemblies throughout the year and wherever else necessary in an age-appropriate and timely manner.

14 In Computing/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.

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 Governors 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.

17 The following list provides examples of unacceptable use of ICT

- Publishing content on the internet (e.g. through personal Facebook accounts or other social media platforms) which is inappropriate and compromises your status as a teacher
- Using personal e-mail addresses to communicate with students.

- Taking photos or videos of students using mobile phones or any other personal digital recording or image capturing devices
- Communicating with children using social networking sites
- Published photographs or videos of students without student or parent consent.
- Allowing students access to material or data which is inappropriate for their use.

18 All staff have a responsibility to take appropriate action to safeguard themselves and students in relation to the use of IT. Staff will carry out the following actions when using IT in the school environment:

- Monitor student activities which involve the use of ICT
- Report any cyber bullying to Head of Year
- If cyber bullying takes place using school ICT equipment, report this to the IT Support team or E -Safety Co-ordinator who can take appropriate action
- If e-mailing students as part of learning activities, use a school email account and restrict the content of messages to the learning activity
- Check any media such as videos prior to using them in class to assess whether it is acceptable and appropriate. Seek advice if uncertain
- Lock school computers or laptops when away from them to avoid misuse by others and giving access to sensitive information

19 To support the remote learning provision Alderbrook began providing during the Covid-19 outbreak, a remote learning agreement for teachers has been drawn up to provide guidance to staff. (See Appendix C).

20 School e-mail should only 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.

21 Misuse of internet facilities may constitute gross misconduct which can result in a final written warning or dismissal. If a member of staff is concerned about any aspect of their Internet use in school, they should discuss this with the Headteacher, Network Manager or E- Safety Co-ordinator to avoid any possible misunderstanding. Information and guidance will be provided to staff in a clear and simple format.

Data Protection

22 In accordance with the general data protection regulations (GDPR), staff are obliged to use, process and store data in line with the seven 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.

23 The Seven Principles of GDPR

- 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

24 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.

25 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 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. In situations where offensive content has been posted on social media sites the school would as part of its immediate response send the link to *UK Safer Internet Centre* to ensure removal of the offensive content from the site.

26 In the event that Remote Learning is required a remote learning agreement has been drawn up to make students and parents aware of the expectations when working away from school in order to safeguard students and staff. Parents will receive a letter advising them of the agreement and providing guidance on e-safety at home and on how to support their children's remote learning (see Appendix B).

Managing published content

27 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.

28 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.

29 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.

30 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.

Filtering, Supervision and Monitoring

31 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 IT Support staff in discussion with the DSL and senior management team.

e-filtering

32 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.

33 Staff, students and governors 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.

34 The network infrastructure (wired and wireless) is protected from internet penetration by the School Next Generation firewall (NGFW) . Wireless access is protected for domain devices and domain users. A guest SSID (wireless network) is provided to allow school visitors filtered internet access only.

e-supervision

35 Classroom computer management is conducted through NetSupport School which provides real-time viewing of student screens, program white-list and black-list and Internet white- list and black-list.

e-monitoring

36 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.

Management of emerging technologies

37 Emerging technologies will be examined for their educational benefit. Then a risk assessment and appropriate staff training will be carried out before use is allowed.

Appendix A

Lesson structure

Lesson 1: Activating school accounts

Learning Objectives

- To know how to use privacy settings/setting passwords
- To be able to keep sensitive information about yourself hidden

Lesson 2: Cyberbullying

Learning Objectives

- To define the term cyberbullying
- To describe the different forms of cyberbullying
- To evaluate the impact of cyberbullying on young people

Lesson 3: Personal Data

Learning Objectives

- To define the term personal data
- To identify ways in which personal data can be exploited
- To explain ways to protect personal data

Lesson 4: Personal Data

Learning Objectives

- To define the term online grooming
- To describe ways in which online grooming can occur
- To evaluate strategies to prevent online grooming

Lesson 5: Fake News

Learning Objectives

- To define the term “fake news”
- To be able to pick out features of a fake news article/report
- To evaluate the consequences of fake news on society

Lesson 6: Trolling

Learning Objectives

- To define the term trolling
- To identify examples of trolling
- To consider the consequences for trolls and their victims

Appendix B

Students Acceptable Use Policy

- I will be respectful towards my teachers and other students at all times.
- School provided ICT facilities are provided as a privilege not a right, therefore I will use them in a sensible and mature manner, following instructions at all times
- If a device is not functioning correctly I will report it to the class teacher and not attempt to fix it myself, this includes all leads, data and power sockets
- No food or drink are allowed by any ICT equipment for health and safety of myself and others
- I understand that restrictions are in place to prevent accessing or installing unauthorised software, accessing inappropriate websites and accessing unauthorised accounts and documents
- I will not use ICT equipment in an inappropriate manner, attempt to access inappropriate material, attempt to circumvent restrictions or attempt to access any accounts, sites or documents I am not authorised for
- I will not physically damage any ICT equipment or peripherals (including mice and keyboards)
- I will not use ICT equipment or facilities in an abusive or threatening manner towards anyone else at any time for any reason and will report any offensive or worrying messages to a member of school staff immediately
- I will not copy anything from Class Charts, school emails, Microsoft Teams or other platforms used by teachers, and place on any other on-line platform or social media.
- I will not record any part of any audio or video call (Key Stages 4 and 5)
- I agree that my teacher may record any live video calls to ensure the safety of all pupils and staff involved (Key Stages 4 and 5)
- If emailing teachers, I will use my school email (unless in an emergency if I can't find my password)
- I will maintain the same standards of behaviour when using technology at home as I would do in school knowing that all activity on devices and in the cloud is monitored by school.
- If I am involved in a live lesson, I will keep my camera switched off and will never record this for myself.
- I understand that only the teacher will have the ability to schedule any form of live lesson, and this will be by invite only so that the students joining are monitored.
- I understand that deliberately breaking any of this agreement, will result in a sanction.
- If I feel unsafe in any way when using ICT I will speak to a member of staff about my concerns – I will not keep them to myself

Appendix C

Remote Learning Agreement for Teachers

- Communicate within school hours as much as possible.
- Communicate through media agreed by SLT: school email accounts, Class Charts, Microsoft Teams.
- Never use personal email accounts for correspondence with staff, parents/carers or students.
- Do not share personal information with students, such as personal email, telephone numbers or address.
- Check any media such as videos or website links, prior to using them in class to assess whether it is acceptable and appropriate. Seek advice if uncertain.
- No one-to-one tuition using cameras, to safeguard staff and students.
- If making phone calls home, direct the call to the parent/carer. If you speak to the child, make sure the parent/carer is present. Ensure your private number is blocked, and that the call is logged using the school's system.
- Handle all school data with due care and attention, taking additional precautions to protect all student data in these unusual circumstances, such as logging out of any shared data bases and mark books when working from home. Find the GDPR Policy on the school website.
- **If using Microsoft Teams, have a 'test' run with a colleague first, and make sure you are familiar with the features that are available, a**s a minimum, make sure you know how to mute microphones and turn off cameras. This will give you more control over what you share with others. Find out how to tell if the call is being recorded, what exactly is recorded (audio, pictures, messages), and who can access the recordings. Follow guidance from the Teams help resources, and as directed by school. No cameras of students should be used. If a teacher is conducting a live lesson, another teacher should also be present.
- **If on Teams, and you enable your own camera, the following should apply:**
    - Sit against a neutral background, never in your bedroom. Use blurring or an appropriate built in background filter.
    - Dress appropriately
    - Double check that any other tabs open in their browser would be appropriate for a child to see
    - Use professional language

***References**: DFE Government Guidance – Safeguarding and Remote Education. Alderbrook School Policies: Learning and E safety, Safeguarding and Child Protection Policy*