E-Safety Policy

Rational
Information Technology should form a central part of the curriculum as it plays an ever-increasing role in children's lives. Information Technology should be recognised as a means to support learning across the curriculum.

Aims
To protect pupils from online access to undesirable materials
To filter out any undesirable materials
To ensure the safety of any child using the Internet and or email
To monitor children's use of the Internet
To ensure all staff are appropriately trained to teach e-safety

USE OF COMPUTERS AND THE INTERNET
All children, whatever their needs, will have access to a range of up-to-date technologies in classrooms. Computing is a life skill and should not be taught in isolation. Information and Communications Technology covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of Computing within our society as a whole. Currently the internet technologies children are using both inside and outside of the classroom include:
• Websites
• Learning Platforms and Virtual Learning Environments
• Email and Instant Messaging
• Chat Rooms and Social Networking
• Blogs
• Podcasting
• Video Broadcasting
• Music Downloading
• Gaming
• Mobile/Smart phones with text, video and/or web functionality
• Other mobile devices with web functionality

WHOLE SCHOOL APPROACH

E-SAFETY IN THE CURRICULUM

Computing and online resources are increasingly used across the curriculum. We believe it is essential for e-safety guidance to be given to the pupils on a regular and meaningful basis.

Children will have supervised access to Internet resources
• Staff must preview any recommended sites before use. Particular care must be taken when using search engines with the children as these can return undesirable links.
• Raw image searches are discouraged when working with pupils.

• If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work. Parents need to be advised to supervise any further research.
• Our internet access is controlled through the Integra web filtering service.
• Staff and pupils are aware that school-based email and internet activity can be monitored and explored further if required.
• If staff or pupils discover an unsuitable site, the screen must be switched off / closed and the incident reported immediately to a computing leader, technician or member of SLT.
• It is the responsibility of the school, by delegation to the network manager, to ensure that antivirus protection is installed and kept up to date on all school machines.

All members of the school community have a responsibility for promoting and supporting safe behaviours in their classrooms and follow school e-safety procedures. The computing leaders will ensure they are up to date with current guidance and issues through organisations such as South Gloucestershire, SWGfL, CEOP (Child Exploitation and Online Protection), Integra advice and Child Net. They then ensure that the Headteacher; Heads of School and Governors are updated as necessary.

All staff should be familiar with the school's policy including:
• safe use of email
• safe use of the Internet
• safe use of the school network, equipment and data
• safe use of digital images and digital technologies, such as mobile phones and digital cameras
• publication of pupil information/photographs on the school website
• procedures in the event of misuse of technology by any member of the school community
• their role in providing e-safety education for pupils.

DEVELOPING E-SAFETY SKILLS

Children have the opportunity to develop their Internet skills in all subject areas. They are taught how to use the Internet safely. Termly, the computing lessons will start with an E-safety lesson and the use of the SMART rules will be discussed at the start of each computing lesson.

During E-safety sessions and when appropriate across all areas of the curriculum children will be taught
.
• The dangers of technologies that may be encountered outside school
• Copyright and respecting other people's information, images, etc. through discussion, modelling, and activities
• The impact of online bullying and how to seek help if they are affected by these issues
• How to seek advice or help if they experience problems when using the internet and related technologies (cyber bullying)
• How to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the computing curriculum
• About the risks inherent in using social media, particularly if they are contacted by people they do not know.

MANAGING INTERNET ACCESS

Staff are reminded/updated about e-safety regularly and new staff and students receive information on the school's acceptable use policy as part of their induction.

As a duty of care, teaching staff will inform a member of the Senior Leadership Team or a member of the Computing Team if they have evidence of children using websites or applications that are not appropriate for them. This includes sites and applications that children are using at home.

The Computing Team or SLT will follow this up with both the child and parent and report the child to the company concerned.

At Almondsbury CE Primary School, we understand the responsibility to educate our pupils on e-safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom. 'Schools are finding that a blocking and banning approach, which merely limits exposure to risk, may no

longer be a sustainable approach… Schools need to focus on a model of empowerment; equipping children with the skills and knowledge they need to use technology safely and responsibly, and managing the risks' (Becta Safeguarding Children Online Feb 2009)

FILTERING AND MONITORING STANDARDS

We provide a safe environment to learn and work, including when online. Filtering and monitoring are both important parts of safeguarding pupils and staff from potentially harmful and inappropriate online material.
• The Designated Safeguarding Lead (DSL) is responsible for ensuring the standards are met.
• Integra is Almondsbury's External Service Provider.

It is the responsibility of the DSL and the SLT to:
• procure filtering and monitoring systems
• document decisions on what is blocked or allowed and why
• review the effectiveness of your provision
• oversee reports

They are also responsible for making sure that all staff:
• understand their role
• are appropriately trained
• follow policies, processes and procedures
• act on reports and concerns

The DSL takes lead responsibility for safeguarding and online safety, which could include overseeing and acting on:
• filtering and monitoring reports
• safeguarding concerns
• checks to filtering and monitoring systems

The IT service provider should have technical responsibility for:
• maintaining filtering and monitoring systems
• providing filtering and monitoring reports
• completing actions following concerns or checks to systems

The IT service provider should work with the senior leadership team and DSL to:
• procure systems
• identify risk
• carry out reviews
• carry out checks

The filtering and monitoring provision at Almondsbury is monitored annually. Our filtering system blocks harmful and inappropriate content, without unreasonably impacting teaching and learning. There are effective monitoring strategies in place that meet the safeguarding needs of the school.

Further information can be found at https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges/filtering-and-monitoring-standards-for-schools-and-colleges.

Email
The use of email within school is an essential means of communication for staff. In the context of school, email should not be considered private. Educationally, email can offer significant benefits including; direct written contact between schools on different projects, be they staff-based or pupil-based, within school, between schools or international.

We recognise that pupils need to understand how to style an email in relation to their age.
• Pupils are introduced to email as part of the Computer Science Scheme of Work.
• The school gives staff their own email account, to use for all school business. This is to minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed.
• Under no circumstances should staff contact pupils or parents using personal email addresses.

• Pupils may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes.
• The forwarding of chain letters is not permitted in school.
• Pupils must immediately tell a teacher/trusted adult if they receive an offensive email.
• All pupils must use appropriate language in emails and must not reveal personal details of themselves or others in email communication, or arrange to meet anyone.
• Staff must inform a member of SLT if they receive an offensive email.
• Staff professional communication via email must only be done through a school email account.
• Response to parents' email must be done reasonably ideally within a 48-hour period and within acceptable working week day hours.
•Staff may respond to email outside of these hours at their own professional discretion.

PUBLISHING PUPILS IMAGES AND WORK

On a child's entry to the school, all parents/guardians will be asked to give permission for their child's photo to be taken and to use their child's work/photos in the following ways:
• on the school web site
• in display material that may be used in the school's communal areas
• in display material that may be used in external areas, i.e. exhibition promoting the school
• general media appearances, e.g. local/national media / press releases sent to the press highlighting an activity (sent using traditional methods or electronically.)

Pupils' names will not be published alongside their image and vice versa without permission from the parents. Full names will not be published.

SOCIAL NETWORKING AND GAMING

We block/filter access for pupils to social networking sites. Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.
• Pupils will be advised never to give out personal details of any kind which may identify them or their location.
• Parents will be given relevant information as to age ranges for relevant social media sites and games to guide them in their children's appropriate use.

Many websites have an age restriction of 13 and over, and are therefore not suitable for any Primary aged children.

The following applications/sites are examples and are not an exhaustive list.

Application/Site	Age Restriction
Musical.ly	age limit 13+
Fortnite	age limit 12+
Instagram	age limit 13+
Facebook	age limit 13+
WhatsApp	age limit 13+
Snapchat	age limit 13+
YouTube channel	age limit 13+
Minecraft	has two age limit settings 7+ & 13+

All users need to be aware of the range of risks associated with the use of these Internet technologies.

MANAGING EMERGING TECHNOLOGIES

Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed.
• Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.
• Classes have been issued with an iPad to use for school photography, assessment notes, emails, music and educational applications.
• Personal mobile phones should not be used for taking photographs of children.

Data protection (GDPR) Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018. The Act requires schools to:
• Keep personal information safe and secure.
• Protect personal information from misuse.
• Process data securely and confidentially.
• Ensure that all the information they hold about data subjects is accurate.
• Only collect and hold data for its intended purpose.
• Give data subjects control over the use of their personal data.
• Ensure that third parties with whom they share data also process data securely.

All GDPR requirements are followed in accordance with the school's Data Protection policy. The Act requires anyone who handles personal information to comply with important data protection principles when treating personal data relating to any living individual. The Act grants individuals rights of access to their personal data, compensation and prevention of processing. Further guidance can be found at https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted.

RESPONDING TO E-SAFETY INCIDENTS OR COMPLAINTS

As a school we will take all reasonable precautions to ensure e-safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. The school cannot accept liability for material accessed, or any consequences of Internet access.

Complaints relating to e-safety should be made to a member of the Senior Leadership Team. Any complaint about staff misuse must be referred to the Headteacher.
• All users are aware of the procedures for reporting accidental access to inappropriate materials. Any breach must be reported immediately.
• Deliberate access to inappropriate materials by any user will lead to the incident being logged and, depending on the seriousness of the offence; investigation by the Headteacher / LA, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences.
• Pupils and parents will be informed of the complaints procedure.
• Parents and pupils will need to work in partnership with staff to resolve issues.

CYBERBULLYING

Cyberbullying is the use of computing, particularly mobile phones and the internet, to deliberately upset someone else. The whole school community has a duty to protect all its members and provide a safe, healthy environment. The Educations and Inspections Act 2006 states that Head teachers have the power 'to such an extent as is reasonable' to regulate the conduct of pupils when they are off site.

Although bullying is not a specific criminal offence in the UK law, there are laws that can apply in terms of harassing or threatening behaviour and can include (but not limited to):
• excluding a child from online games, activities or friendship groups
• sending threatening, upsetting or abusive messages
• creating and sharing embarrassing or malicious images or videos
• 'trolling' - sending menacing or upsetting messages on social networks, chat rooms or online games
• voting for or against someone in an abusive poll
• setting up hate sites or groups about a particular child
• creating fake accounts, hijacking or stealing online identities to embarrass a young person or cause trouble using their name.

PREVENTING CYBERBULLYING

It is important that we work in partnership with pupils and parents to educate them about Cyberbullying as part of our e-safety curriculum. They should:
• understand how to use these technologies safely and know about the risks and consequences of misusing them.
• know what to do if they or someone they know are being cyberbullied.
• report any problems with Cyberbullying.

If they do have a problem, they can talk to the school, parents, the police, the mobile network (for phone) or the Internet Service Provider (ISP) to do something about it.

Additional online advice on how to react to Cyberbullying can be found on https://www.kidscape.org.uk/ and www.wiredsafety.org

SUPPORTING THE PERSON BEING CYBERBULLIED

Support will be given in line with the behaviour policy.
• Give reassurance that the person has done the right thing by telling someone and inform parents.
• Make sure the person knows not to retaliate or return the message.
• Help the person keep relevant evidence for any investigation (taking screen capture shots, not deleting messages).
• Check the person knows how to prevent it from happening again e.g. blocking contacts, changing contact details.
• Take action to contain the incident when content has been circulated: remove content, contact the host (social networking site) to get the content taken down, use disciplinary powers to confiscate phones that are being used to cyberbully – ask the pupil who they have sent messages to.

INVESTIGATING INCIDENTS

All cyberbullying incidents must be recorded on CPOMS. We will then investigate the matter fully as we would with any other bullying incident (refer to behaviour policy and anti-bullying policy).

WORKING IN PARTNERSHIP WITH PARENTS

Parents/carers are asked to read through and sign Acceptable use of Computing agreements on behalf of their child on admission to school (see appendix 1).
• Parents/carers are required to decide as to whether they consent to images of their child being taken/used in the public domain (e.g. on school website).
• A partnership approach with parents will be encouraged. This includes parents evenings with suggestions for safe home Internet use.
• Advice on filtering systems and educational activities that include safe use of the Internet will be made available to parents.

SCHOOL WEBSITE

The school website enables the school to communicate effectively with parents and the wider community. The website contains pertinent information about the school, its policies, procedures, routines and celebrates its successes. The Computing team will oversee the updating of the website along with the Headteacher and the company managing the website e4education.

DEVELOPING AND MONITORING THE E-SAFETY CURRICULUM

The e-safety curriculum is subject to frequent change due to the advances in technology. The implementation of the plans will be monitored by the Computing team. Teaching of e-safety to all children will be monitored through observations and monitoring of planning and assessments by the Computing subject leader and the Headteacher.

Almondsbury C of E Primary School Staff (and Volunteer) Acceptable Use Policy Agreement

Policy Context

The Internet and other technologies are powerful tools, which open up new opportunities for everyone. They can stimulate discussion, promote creativity and promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to good, safe access to digital devices and the Internet. This Acceptable Use Policy is intended to ensure that:

- Staff and volunteers are responsible users and stay safe while using technologies for educational, personal and recreational use.
- School computer systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- Staff are protected from potential risk from the use of electronic devices in their everyday work and work to ensure that young people in their care are safe users.

Acceptable Use Policy Agreement

I understand that I must use the school digital systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the digital systems and other users.

Keeping Safe

- I know that the school will monitor my use of the ICT systems, email and other digital communications.
- I will only use my own usernames and passwords which I will choose carefully so they cannot be guessed easily.
- I will not use any other person's username and password.
- I will ensure that I will lock my devices when I am not using these or log out.
- I will not engage in any online activity that may compromise my professional responsibilities or compromise the reputation of the school or its members.
- I understand that data protection requires that any personal data that I have access to must be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose it to an appropriate authority.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the school personal data policy.
- Where personal data is transferred outside the secure school network, it must be encrypted.
- I will not try to bypass the filtering and security systems in place.
- I will only use my personal ICT in school for permissible activities and I will follow the rules set out in this agreement. I will ensure that any such devices are protected by up-to-date anti-virus software and are free from viruses.

Promoting Safe Use by Learners

- I will model safe use of the Internet in school.
- I will educate young people on how to use technologies safely according to the school teaching programme.
- I will take immediate action in line with school policy if an issue arises in school that might compromise learner, user or school safety or if a child reports any concerns.
- I will not use personal devices to take photos. I will only take any photos or images of children on school devices such as ipads, laptops and upload these to the drives as soon as possible. These will not be used for any other purposes.

Communicating

- I will communicate online in a professional manner and tone. I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will only communicate with students / pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner.

- I will be aware that any communication could be forwarded to an employer or governors.
- I will not use chat and social networking sites in school.

Research and Recreation

- I will not upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others.
- I will not (unless I have permission) make large downloads or uploads. I will not download or access any materials that have not been approved by the school or already on the system.
- I know that all school ICT is primarily intended for educational use and I will only use it for this purpose.

Sharing

- I will not access, copy, remove or otherwise alter any other user's files, without their permission.
- I will ensure that I have permission to use the original work of others in my own work and will credit them if I use it.
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).
- I will only take images / video of pupils and staff where it relates to agreed learning and teaching activities and will ensure I have parent / staff permission before I take them.
- If these are to be published online or in the media, I will ensure that parental / staff permission allows this.
- I will not use my personal equipment to record images / video unless I have permission to do so.
- I will not keep images and videos of students stored on my personal equipment unless I have permission to do so. If this is the case, I will ensure that these images cannot be accessed or copied by anyone else or used for any purpose other than that I have permission for and I will delete any images/videos as soon as they have been used for the purpose for which I had permission.
- Where these images are published (e.g. on the school website) I will ensure it is not possible to identify the people who are featured by name or other personal information.

Buying and Selling

- I will not use school equipment for online purchasing and selling unless I have permission to do so.

Problems

- I will immediately report any illegal, inappropriate or harmful material or incident I become aware of, to the E-safety co-ordinator or Headteacher.
- I will not install or store programmes on a computer unless I have permission.
- I will not try to alter computer settings, unless this is allowed in school policies.
- I will not cause damage to ICT equipment in school.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.

I understand that these rules are in place to enable me to use ICT safely and that if I do not follow these I may be subject to disciplinary action. I agree to use ICT by these rules when:

- I use school ICT systems at school or at home when I have permission to do so
- I use my own ICT (when allowed) in school
- I use my own ICT out of school to use school sites or for activities relating to my employment by the school

Staff / Volunteer Name	
Signed	
Date	

Almondsbury C of E Primary School Rules for Keeping Safe with ICT

Keeping Safe

- I will not use ICT in school without permission from my teacher.
- I will choose my usernames and passwords carefully to protect my identity and I will not share them.
- I will not ask computers to remember my password.
- I must keep my personal details and those of others private.
- I will not visit unsafe sites or register for things I am not old enough for.
- I will logoff sites when I have finished.

Communicating

- I know that I need to be polite and friendly online.
- I know that others may have different opinions and that I should respect them.
- I am careful about what I send as messages can be forwarded on to my parents or headteacher.
- I know that I must have permission to communicate online and will make sure my teacher / parents know who I communicate with.
- I will not arrange to meet an online friend without permission.
- I will not open messages if the subject field is not polite or if I do not know who it is from.

Research and Fun

- I will use clear search words so that I find the right information.
- I know that some content may not be filtered out.
- I will double-check information I find online.

Sharing

- I will not use anyone else's work or files without permission.
- Where work is protected by copyright, I will not try to download copies.
- I will not take or share pictures of anyone without their permission.
- I know that anything I put up on the Internet can be read be anyone.

Buying and Selling

- I can tell if a site is trying to sell something.
- I know that I should not buy or sell anything online without permission.

Problems

- I will not try to change computer settings or install programs.
- I will tell a teacher if I find anything on a computer or message that is unpleasant or makes me feel uncomfortable.
- I will not damage equipment and will tell a teacher if equipment is broken or not working.

I agree to use ICT by these rules when:

- I use school ICT or my own in school (when allowed)
- I use my own ICT out of school to use school sites

My Name is

My Class teacher is

Signed

Date