Aldington Primary School

Appendix 2

Online Safety and Acceptable Use Policy 2023-2024

All staff should have access to this policy and sign to the effect that they have read and understood its content.

Prepared by: Selina Eyles	Date: 05/12/2023
Approved by: Ben Dawson	Date: 05/12/2023
To be reviewed:	Date: December 2024

Nurture and Challenge

Rationale

It is the duty of the school to ensure that every child in their care is safe, and the same principles should apply to the 'virtual' or digital world, as would be applied to the real world. Increasingly, children are accessing material through online sources (some of which may not be age appropriate). It is, therefore essential to address this and encourage a lifestyle which incorporates a healthy balance of time spent using technology and knowing what is appropriate for their age range.
This policy, supported by the Acceptable Use Policy (AUP, appendix 1) for staff, governors, visitors and pupils exists to protect the interests and safety of the whole school community and aims to provide clear advice and guidance on how to minimise risks.

The Technologies

At Aldington we understand that ICT has an increasing role in the lives of children and adults. New technologies are enhancing communication and the sharing of information. Current and emerging technologies used in school and, in many cases, used outside of school, by the children include:

- The Internet
- E-mail
- Instant messaging
- Blogs
- Social networking sites
- Chat rooms
- Gaming sites
- Text messaging and picture messaging
- Video calls
- Podcasting
- Online communities via games consoles
- Mobile internet devices such as smart phones and tablets.

Whole School Approach to the safe use of ICT

At Aldington, creating a safe ICT learning environment includes three main elements:

1. An effective range of technological tools which are filtered and monitored;
2. Policies and procedures, with clear roles and responsibilities;
3. A progressive online safety education programme that is taught across the school involving pupils, staff and parents.

Staff Responsibilities

Online Safety is recognised as an essential aspect of teaching and learning across the school. We aim to embed safe practices into the culture of the school to allow children to feel, act and respond safely when using ICT. All staff are responsible for teaching the children skills to use ICT appropriately. The staff will be expected to discuss online safety issues before the use of any form of technology, in all areas of the curriculum. Staff are encouraged to create a 'talking culture' in order to address any online safety issues which may arise in the classroom or around the school on a daily basis.

All members of staff are also responsible for ensuring the children know and understand the school rules regarding our use of the Internet (see appendix 4) and practice these when using the Internet. As Computing Lead, our school Online Safety Coordinator is Anna Ransley. As designated safeguarding lead Ben Dawson can also be referred to if necessary. The Online Safety coordinator ensures they are up to date with online safety issues and guidance through liaison with staff members and through organisations such as The Child Exploitation and Online Protection (CEOP) and 360 Safe. The Online Safety coordinator ensure the Head Teacher, Senior Management and Governors are updated when needed.

Staff Awareness

- All staff receive regular information and training on online safety issues in the form of in-house training and meeting time.
- New staff receive information on the school's AUP as part of their induction.
- All staff are made aware and reminded of individual responsibilities relating to the safeguarding of children, within the context of online safety and know what to do in the event of misuse of technology by any member of the school community.
- Online safety records of concern are completed by staff as soon as incidents occur and are reported directly to the school safeguarding team (see appendix 3).
- All staff are expected to refer to school rules and online safety guidelines throughout their learning through ICT.

All staff working with children are responsible for demonstrating, promoting and supporting safe behaviour in their classroom, following school Online Safety procedures. These behaviours are summarised in the AUP (appendix 1) which must be signed and returned before use of technologies in the school.

Internet

- Aldington Primary School uses a "filtered" Internet Service via EiS which will minimise the chances of pupils encountering undesirable or unsafe material.
- Staff and pupils have access to the internet through the school's fixed and mobile internet technology.
- Staff will only email school-related information using their @aldington.kent.sch.uk address and not personal accounts.
- Staff will preview any websites before recommending them to pupils.
- Staff will either provide appropriate links to websites or teach children appropriate methods of searching via the Internet.
- If internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher.
- The CEOP Report Abuse button is available on the school website. Teachers are to make children aware of this and when it is appropriate to use it.

- If staff or pupils discover an unsuitable site, the screen must be switched off immediately and the incident reported to the online safety coordinator. The device and username will need to be recorded for the purpose of safety.
- Staff and pupils are aware that school based email and internet activity is monitored and can be explored further if required.
- Pupils using the World Wide Web are expected to not deliberately seek out offensive materials. Should a pupil encounter any such material accidentally, they are expected to report this to the teacher who can seek advice from the online safety coordinator.
- Pupils are expected not to use any rude or offensive language in their email communications and contact only people they know or those the teacher has approved.
- They are taught communication etiquette in email and are expected to follow these rules. No personal information such as phone numbers and addresses should be given out and no arrangements to meet someone made, unless this is part of an approved school project.
- Pupils consistently choosing not to comply with these expectations will be warned, and subsequently, may be sanctioned following the school's behaviour policy.
- A copy of the online safety rules (appendix 4) are displayed in all areas where ICT is being used (classrooms). Pupils will be asked to sign these rules as an agreement, ensuring the awareness of the expectations. A copy has also been sent home to parents to ensure that these key messages are reinforced at home.
- The Internet use agreement will also appear when children log in to the networked computers in school. They are required to click to agree to the policy before they are allowed to use the computers.

Passwords:

- Children in Key Stage 1 will be taught to log on to the school network using their own name. Children will be encouraged to do this and reminded of the consequences of not complying with this rule.
- Children in Key Stage 2 will be introduced to a progressive password system that allows the children to create their own memorable password in Year 6. The children will be reminded of the rules creating passwords.
- Use a strong password (Strong passwords are usually eight characters or more containing upper and lower case letters, as well as numbers.)
- Passwords should not be written down.
- Passwords should not be shared with other children or staff.

Mobile Technology

- School iPads and laptops should always be used for school-related reasons.
- Apps will need to have been researched and approved by the adult requesting them.
- Mobile devices should not leave the school premises.
- All devices need to be accounted for at the end of each day.
- Mobile technology such as iPads and laptops are stored in a locked trolley/ charging unit. Members of staff (not visitors or children) should sign in/out the key for these devices before and after each use.
- When devices are not being used, staff should ensure that they are returned to prevent unauthorised access.

- No personal devices belonging to staff or children are to be used during lessons at school. If staff bring in their own devices such as mobile phones, these are to be used during break times and kept on silent. These devices should be out of sight to children.
- If pupils bring in mobile phones (for the purpose of safety if they walk to and from school alone), they should be switched off and placed in the basket in the Office and this will remain the responsibility of the child in case of loss of damage. Any children not following these rules will be dealt with using the school's behaviour policy.

Data Storage

- Staff are expected to save all sensitive data onto our secure online platform Kent Learning Zone (KLZ) or onto our staff shared area on our computers.
- Removable media (USB memory sticks, pen drives, CDs, portable drives) are allowed but only for data such as planning, resourcing etc. where children's names and sensitive information are not used.
- EHCP's, assessment records, pupil medical information and any other data related to pupils or staff should not be stored on personal memory sticks.
- All staff must agree to and sign the Data Security guidelines (see appendix 2).

Social Networking Sites

- Use such sites with extreme caution, being aware of the nature of what you are publishing online in relation to your professional position. Do not publish any information online which you would not want your employer to see.
- Under no circumstances should school pupils or parents, past or present, be added as friends, unless known to you as a friend or relative prior to your appointment.
- Staffs role in school requires a high degree of professionalism and confidentiality.
- Permission from parents to allow children to be photographed and posted on the school's Twitter page must be obtained before any images are posted.

Digital Images

- Use only digital cameras and video cameras provided by the school and under no circumstances use personal equipment such as digital cameras or camera phones to store images of children.
- Ensure you are aware of the children whose parents/carers have not given permission for their child's image to be used in school/on the school website/on the school Twitter account. An up to date copy is present in the class folders and the school office.

Members of staff who breach the acceptable use policy may face disciplinary action. A misuse or breach of this policy could result in criminal or civil actions being brought against you.

Providing a comprehensive online safety education to pupils and parents

Staff	• All staff working with children must share a collective responsibility to provide online safety to pupils and to promote online safety in their own actions. • All staff will use the 'South West Grid for Learning' digital literacy scheme to deliver high quality online safety lessons. • Online Safety will be taught across the curriculum whenever pupils and staff are using ICT. • The Computing Coordinator will lead an assembly each year highlighting relevant online safety issues and promoting safe use of technologies. • When using any technological devices to support learning in class, members of staff will acknowledge the school's online safety rules where appropriate and remind pupils how to report a problem if any were to arise. • Staff will encourage positive and responsible technology use by using praise and reward systems for pupils who demonstrate a consistent, clear understanding of online safety. • The school website will be updated regularly with relevant e-safety resources for parents and pupils.
Pupils	• Online Safety will be taught as an individual lesson once a term apart from Term 3, where all pupils will engage with 'Safer Internet Day'. Within these lessons pupils will be taught how to assess and manage online risk for themselves and will have a comprehensive understanding of what to do if an issue arises. • During Online Safety sessions pupils will also be invited to discuss strategies for the school community's online safety and how their views can support it. • Pupils will know where to find the online safety rules in their classroom and will have a clear understanding of them.
Parents	• Staff will remind parents of the online safety rules throughout the year. This will be through letters, workshops, open afternoons and meetings. • During at least one open afternoon a year, pupils will have the opportunity to educate parents through various classroom activities. • During online safety workshops parents will be invited to discuss and develop the provision of online safety at home and within the school community.

Maintaining the security of the school IT Network

Martin Page (IT technician) maintains the security of the school network and is responsible for checking on a regular basis that the virus protection is up to date on all technologies. However, it is also the responsibility of the IT users to uphold the security and integrity of the network.

Complaints procedure

Online safety is a high priority at Aldington Primary School, therefore any complain or concern relating to online safety is made by a member of staff, child, parent/carer then it will be considered and prompt action will be taken.
Complaints should be addressed to the online safety coordinator in the first instance, who will undertake immediate action to investigate and liaise with the leadership team; including the designated safeguarding lead and members directly involved in the issue raised.
Incidents of online safety concern will be recorded using a Record of Concern proforma (appendix 3) and reported to the school's designated safeguarding officer in accordance with the school's Child Protection Policy. Any complaints of cyberbullying are dealt with in accordance to the school's Anti-Bullying Policy.

Monitoring

The Head Teacher/Deputy Head Teacher or any other authorised members of staff may inspect or monitor any ICT equipment owned or leased by the school at any time, without any prior warning.
Monitoring may include: intercepting, accessing, inspecting, recording and disclosure of telephone calls, e-mails, instant messaging, internet/intranet usage and any other electronic communications involving employees without prior consent, to the extent permitted by law. This may be to confirm or obtain School business related information; to confirm or investigate compliance with School policies, standards and procedures, to ensure the effective operation of School ICT, for quality control or training purposes, to comply with a Subject Access Request under the Data Protection Act 1998, or to prevent or detect crime.

Breaches of Policy

Any policy breaches are grounds for disciplinary action in accordance with the School Disciplinary Policy. Policy breaches may also lead to criminal or civil proceedings.

Incident Report

All security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the school's Designated Safeguarding Person Ben Dawson or the Computing Lead Anna Ransley.

Aldington Primary School
ICT Acceptable Use Policy (AUP) for pupils for use at home and at school – Our Charter for Good Online Behaviour

I promise – to only use the school computers and technologies for schoolwork or homework (during homework club) that the teacher has asked me to do.
I promise – not to look for or show other people things that may be upsetting.
I promise – to show respect for the work that other people have done.
I will not – damage the ICT equipment, if I accidentally damage something I will tell an adult.
I will not – waste resources that are limited.
I will not – share any passwords with anyone. If I forget my password, I will let my teacher know.
I will not – share any personal information online with anyone; including my home address, phone number or any pictures of myself or others.
I will not – use other people's work or pictures without permission to do so.
I will not – use other people's usernames or passwords.
I will not – arrange to meet anyone who I have only met on the Internet.
I will not – download anything from the Internet unless my teacher has asked me to.
I will – let an adult know if anyone asks me for personal information.
I will – turn the screen off and tell my teacher or an appropriate adult straight away, if I see anything I am unhappy with.
I will – let my teacher or parent know if anyone says or does anything to me that is hurtful or upsets me, makes me feel worried or uncomfortable.
I will – let my teacher know if I see bad language or unpleasant pictures on the internet.
I will – be respectful to everybody online; I will treat everybody the way I want to be treated.
I will – ask permission from a member of staff before using the Internet and will only be online when an adult is in the room.
I understand – that some people on the Internet are not who they say they are, and some people can be nasty. I will tell my teacher if I am ever concerned in school or my parents if I am at home. I will always be myself on the Internet and not try to be someone else.
I understand – if I break the rules in this charter there will be consequences of my actions and my parents will be told.

Pupils Name:_____
Signed (Parent/Carer):_____**Date:** _____
Signed (Pupil): _____**Date:**_____

Aldington Primary School
ICT Acceptable use policy for staff, governors and visitors

These rules are designed to protect staff and visitors from online safety incidents and to promote a safe online safety environment for pupils.

- I will only use the school's internet, email, computers, laptops and mobile technologies for professional purposes as required by my role in school.
- I will not disclose my password to anyone else.
- When accessing school emails, KLZ or any other sensitive information relating to Aldington Primary School, I will ensure that it is conducted on a device that has the appropriate security measures i.e. anti-virus, firewall, encryption and log off each site after use.
- I will ensure that any online communications with staff, parents and pupils are compatible with my professional role.
- I will not give out my own personal details to pupils or parents.
- I will send school business emails using my school email address, if I have been provided with one, not my personal email address.
- I will ensure that any data that I store is stored on a secure, encrypted device.
- I will not browse, download, upload or distribute any material which could be considered offensive, illegal or discriminatory.
- Images of pupils will only be taken and used for professional purposes in line with school policy and with the consent of the parent or carer. Images will not be distributed outside of school without the permission of the parent/carer and Head Teacher.
- If it is necessary to bring my own personal devices into school, these will only be used during non-contact time, without pupils.
- **I will report any online safety concerns I have to the designated safeguarding officer (Ben Dawson) immediately using the 'Online Safety Record of Concern'.**
- **Mobile phones will be out of sight and switched to silent at all times during the school day.**
- **I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.**
- **I will support the school's online safety policy and support and encourage pupils to be safe and responsible in their use of ICT and related technologies.**

I understand the procedures and agree to follow them with immediate effect.

Print name:_____ **Signed:**_____ **Date:** _____

Aldington Primary School
Data Security

Following a review of procedures in place to store sensitive data in line with National recommendations the following practice is to be adhered to:-

Sensitive data consists of any information which is personal to individuals or deemed sensitive or valuable to the school.

All staff are required to only save sensitive data in the following formats:-

- Google Drive
- On an encrypted USB memory stick
- On 'Staff shared' documents on the school server
- Across the school outlook web app email system (@aldington.kent.sch.uk)

This ensures that no legal action can be taken for lost data.
Staff are encouraged to hold all of their data in 'Staff shared' folders on the school server that has a built-in level of encryption. If this is not possible, they are encouraged to save all data onto our learning platform KLZ. The login and password for this account should not be written down anywhere and the KLZ account should be logged out when not in use.
It is the responsibility of the staff to ensure that all sensitive information is only kept in the formats mentioned above and to ensure that access to this information is secured.
Sensitive data should not be sent via email to external agencies, third party agencies or those not employed by the school, unless it is encrypted/password protected.
Failure to follow these guidelines will be treated seriously and may lead to disciplinary procedure.

I understand the procedures and agree to follow them with immediate effect.

Name:_____**Signed:** _____ **Date:** _____