ALDWYN PRIMARY SCHOOL

E-Safety Policy

Reviewed by Governors: Spring 2023

Signed by Governor: J Atherley

Signed by Headteacher: C Beaty

This policy will be reviewed every three years

Review date: Spring 2026

Aldwyn Primary School

E-Safety Policy

Introduction

E-safety is not a computing issue. It may involve the use of computing, but it is about protecting children and young people from harm. Every child at Aldwyn Primary School should be able to participate in an enjoyable and safe environment and be protected from abuse. This is the responsibility of every adult in school. The use of electronic media communication and learning has massively increased in recent years. This offers many benefits and this policy is not intended to curtail that potential for fun, entertainment and learning. However, electronic media also pose some risks for children if they are unaware of the way that information can be used by people with ill-intent to exploit or abuse them.

Child abuse is a very emotive and difficult subject for everyone involved. When electronic media is used to carry out the abuse it can be even more challenging because many people who are significant in the child's life will not be very knowledgeable about the way that the electronic media work. Indeed, it is likely that the child or young person will know more than the adults around them about how to use the media.

Everyone should recognise their responsibility to safeguard the welfare of all children by protecting them from physical, sexual or emotional abuse, neglect and bullying.
This policy reflects the purpose of the Tameside Safeguarding Board
(TSCB) and the content of the TSCB Child Protection Procedures (contained in *Tameside Safeguarding Children Framework*). These include the following principles:

- The welfare of the child is paramount

- All children, whatever their age, culture, disability, gender, language, racial origin, religious beliefs and/or sexual identity, have the right to protection from abuse, including neglect, bullying and exploitation.

- All suspicions and allegations of abuse will be taken seriously and responded to swiftly and appropriately.

When an incident raises concerns both about significant harm and unacceptable use, the first and paramount consideration should always be the welfare and safety of the child directly involved.

At Aldwyn Primary School, we believe that the use of computer technology, including the Internet

- provides instant access to a wealth of up-to-the minute information and resources from across the world, which would not ordinarily be available.
- enables improved communication and facilitates the sharing of data and resources by the use of email, mobile phones, and internet messaging
- provides children and/or young adults with a platform for personalised and independent learning through using the Google Cloud and other cloud-based technology).

However, there are dangers associated with the Internet and emerging new technologies and these have been highly publicised in the media for example:

- Children might inadvertently access content of an unsavoury, distressing or offensive nature on the Internet or receive inappropriate or distasteful emails.
- Children might receive unwanted or inappropriate messages from unknown senders via email or via files sent by Bluetooth. They might also be exposed to abuse, harassment or 'cyber-bullying' via email, text or instant messaging, in chat rooms or on social-networking websites, such as TikTok, Bebo, Facebook, Snapchat etc. (even though the minimum age to subscribe to these is 13/14 years old).
- Chat rooms provide cover for unscrupulous individuals to groom children.

We also recognise that there are social and educational benefits to be derived which far outweigh the risks involved so long as users are made aware of the issues and concerns and receive ongoing education in choosing and adopting safe practices and behaviours. For example:

- Children will be taught a range of strategies (appropriate to their age, ability or stage of development) to help them stay safe when using electronic media as part of the PHSCE curriculum.
- Children are equipped with skills for the future.
- The Internet provides instant access to a wealth of up-to-date information and resources from across the world, which would not be otherwise available.
- The Internet helps to improve children's reading and research skills.
- Email, Instant Messaging and Social Networking helps to foster and develop good social and communication skills.

Procedures for Use of a Shared School Network:

When using a PC / laptop /Chromebook connected to the school network:

- Users must access the school network using their own logons and passwords. These must not be disclosed or shared. From time to time, guest users may log on to the school network using a 'generic' password set up for this purpose.

- Users must respect confidentiality and attempts should not be made to access another individual's personal folder on the network without permission.

- Software should not be installed, nor programmes downloaded from the Internet, without prior permission from the person responsible for managing the network, except for documents, PDFs, forms, etc, that might be downloaded from reputable teaching resource websites or from an organisation such as: DCSF, Ofsted, BBC, etc.

- Our anti-virus software does not scan pen drives or memory sticks for viruses. Some anti-virus does but it can dramatically affect system efficiency. It is the responsibility of users to take all sensible precautions before downloading items from the internet onto any removable media that will be used in school.

- Machines must never be left 'logged on' and unattended. If a machine is to be left for a short while, it must be 'locked.' (Ctrl+alt+del followed by 'lock computer').

- Machines must be 'logged off' correctly after use.

- The school's wireless network is encrypted to prevent outsiders from being able to access it. The password must be stored in a safe and secure place.

Procedures for Use of the Internet and Email:

For safe Internet and Email use:

- All adult users must sign an Acceptable Use Agreement before access to the Internet and email is permitted in the establishment. Guest Users will be given a summary of this agreement so that they know what is acceptable. Parents must sign the ‘Responsible Internet Use’ form which gives permission for children to use the internet and e-mail. Key Stage 2 children must sign the responsible internet use form as they start Year 3. In Key Stage 1 teachers will discuss rules with the children at an appropriate level.

- Users must access the Internet and email using their own logon / password and not those of another individual. Passwords must remain confidential, and no attempt should be made to access another user’s email account.

- The Internet and email must only be used for educational purposes by children. Staff may use the internet and email for professional and educational purposes, and for more personal use. However, they may not use it for on-line gambling or where any content is completely unsuitable for children, e.g. of a sexual nature.

- It is strongly advised that members of staff do not accept friend requests from parents of children in our school on social networking sites. It is also advised that all staff keep their profiles private. No staff should be friends with children. Facebook is not designed for children to use. When someone signs up to Facebook they have to say they are at least 14 years of age. All staff should also think very carefully before posting any messages or photos to a social networking site that might cause embarrassment to themselves or the school if it becomes public knowledge. It is recommended that you do not post anything about any individuals in school that might cause upset or annoyance if it is viewed. Staff should consider whether they would say this to an individual face to face. Staff should not post photographs of other members of staff without their permission. There have been cases locally and nationally where parents or children have seen what has been posted by a member of staff. Staff should also be aware that if someone else posts an offensive message on their wall they can become associated with that offensive message.

- Children must be supervised at all times when using the Internet and email.

- Procedures for Safe Internet use will be clearly displayed in the Computer Suite and in classrooms.

- Accidental access to inappropriate, abusive or racist material by staff or children is to be reported without delay to the person responsible for E-Safety (currently Mr. C. Beaty) or to the Computing Co-ordinator, (currently Mr. N. Bonsall) and a note of the offending website address (URL) taken so that it can be blocked. However, the filtering system in place will almost always prevent access to inappropriate material in the majority of cases. However, staff must bear in mind that no filtering system is 100% effective.

- Internet and email filtering software is installed to restrict access, as far as possible, to inappropriate or offensive content and to reduce the receipt of ‘spam,’ junk or unwanted correspondence. This is to be reviewed and updated regularly.

- Internet and email use can be randomly monitored in accordance with the Data Protection Act. This will be done by the school’s technician or by the Computing co-ordinator.

- Email addresses assigned to individual children are locked into the google apps domain. This means children can neither send or receive external emails unless the relevant domains are “whitelisted”.

- Children must not disclose any information of a personal nature in an email or on the Internet. This includes mobile and home phone numbers, addresses, or anything else which might allow them to be identified. This is also good advice for adult users. In some cases, children and/or young adults might be required to register in order to log into an educational site approved by the school. In this case, ‘cyber names’ (pseudonyms) must be used, which will not allow them to be identified. Any such logins are managed by the school computer administrator.

- All emails sent should be courteous and the formality and tone of the language used appropriate to the reader. No strong or racist language will be tolerated. Sanctions, appropriate to the case, will be imposed on any users who break this code.

- Bullying, harassment or abuse of any kind via email will not be tolerated. Sanctions, appropriate to the case, will be imposed on any users who break this code.

- If users are bullied, or offensive emails are received, this must be reported immediately to a trusted adult or member of staff within the school. Emails received should not be deleted, but kept for investigation purposes. A copy of all emails sent by children are retained for child protection purposes.

- Anti-virus software is used on all machines and this is regularly updated to ensure its effectiveness.

- All email attachments will be automatically scanned before they are opened. E mails with attachments received from unknown senders, and / or if the content of an attachment is not detailed in the body of an email, it should not be opened, but subsequently deleted.

- Although, policies prevent children from downloading and installing unauthorised software, children must not download any files form the internet unless they have specific permission from their teacher.

- All users will be made aware of Copyright law and will acknowledge the source of any text, information or images copied from the Internet. This should be reiterated in any lessons where the Internet is being used for research purposes

Procedures for Use of Chat and Video Messaging.

Children have access to a chat board on Google Classroom and this can be used to provide information and updates about lessons. This chat is monitored by teaching staff. Children also have access to Google Meet but settings in place prevent children from creating their own video and chat sessions. Any such sessions must be initiated by the class teacher and all members of the session are automatically terminated when the chat session is closed.

- Social media sites are automatically blocked for students and children and staff must not access public or unregulated chat rooms.

- Use of Social Networking websites and apps is permitted for use by staff in their own time, e.g. lunch breaks and at home.

Procedures for Use of Cameras, Video Equipment and Webcams:

The school's procedures for safe use of photographic and video equipment are:

- Permission must be obtained from a child's parent or carer before photographs or video footage can be taken. This is done as part of the locality visit permission form which parents sign when their children first enter the school. A register of children who may not be photographed is kept by the current class teacher, and staff must refer to this as a check before displaying children's photographs in school, on the website or in printed newsletters. Any photographs taken containing images of these children must be deleted as soon as possible.

- Photographs or video footage should be downloaded immediately and saved into the P drive – pictures and video. This will be 'password-protected' and accessible only to authorised members of staff. ('Password protected' means accessible only by use of log-on passwords by staff.)

- Staff are encouraged to save digital media to cloud platforms such as OneDrive and Google Drive. This allows digital media to be carefully shared and provides secure and encrypted storage.

- Any photographs or video footage stored on cameras or video equipment should be deleted immediately once no longer needed.

- Any adult using school camera, video recorder or camera phone must transfer and save images and video footage into a secure folder or cloud storage on a school computer as soon as possible. This is to avoid any embarrassment or upset if the item is lost or stolen.

- Children should not accept files sent via Bluetooth to their mobile phones by an unknown individual. If they do, and the content received is upsetting or makes them feel uncomfortable, they should pass this on to a trusted adult straightaway.

- Video conferencing equipment and webcams must be switched off (disconnected) when not in use and the camera turned to face the wall.

- Webcams must not be used by children for personal communication and should only be used with an adult present.

- Children and staff must conduct themselves in a polite and respectful manner when representing the school in a video conference or when corresponding via a webcam. The tone and formality of the language used must be appropriate to the audience and situation.

Procedures to ensure safety of the school’s website:

Aldwyn Primary School has its own website and it is important that the following measures are adhered to in order to ensure the safety of children and staff represented on this:

- Copyright and intellectual property rights must be respected**.** It is important that permission is granted before any files created or owned by another person or company are used on the school website. This applies to photographs, graphics, animations, audio and video clips, clips from TV shows such as those on ‘YouTube,’ scanned images from books, newspapers or magazines, etc.

- Permission must be obtained from parents or carers before any images of children can be uploaded onto the school website. This is done as part of the locality visit permission form which parents sign when their children first enter the school. A register of children who may not be photographed is kept in the staffroom, and staff must refer to this as a check before displaying children’s photographs on the website.

- It is safer not to post images of individuals (especially where children are concerned) onto the school’s website, instead only group photographs may be used. In the case of images for the ‘staffroom’, (where visitors can find out about the staff) children’s drawings may be used instead of photographs.

- Names must not be used to identify individuals portrayed in images uploaded onto the school website. Similarly, if a child or member of staff is mentioned on the website, photographs which might enable this individual to be identified must not appear.

- When photographs to be used on the website are saved, names of individuals portrayed therein should not be used as file names.

Procedures for using mobile phones:

- Children who need to bring mobile phones into school should switch them off before they enter the school playground. Phones should be handed to the office for safe keeping throughout the school day. They should be collected at home time but children must not turn the mobile phone back on until after they leave the school playground.

- The taking of still pictures or video footage of children or staff by a child using a mobile phone is strictly prohibited. In any cases where this should occur, parents will be contacted and the child may be refused permission to bring their mobile phone to school in the future.

- Children found to use a mobile / camera phone for inappropriate or malicious purposes (i.e. for 'happy-slapping,' the sending of abusive or unsavoury images / text messages or files via Bluetooth, the making of hoax, crank or abusive phone calls), will be sent to the Headteacher who will contact their parents. Appropriate sanctions will be invoked.

- Should children or staff in school receive unwanted, unsavoury or hurtful calls, text messages or files sent via Bluetooth they should report this to a trusted adult in the school. Children should also be encouraged to tell their parents, and school and parents would work together to help solve the problem and reassure the child. Any such messages or files received should be kept for investigation purposes and not replied to. The same procedures should be followed if contact is made in any of the afore-mentioned ways by a person unknown to them. In the case of Bluetooth, individuals have the option to refuse a file. If the person is unknown to them, they should be advised not to accept it. If they inadvertently accept inappropriate content, or do so out of curiosity, they must not be afraid to report this and any files should be retained and not deleted.

Procedures for using wireless games consoles:

The use of wireless games consoles is not permitted in school. Their presence might lead to instances of theft, but as children can also connect to the Internet and play against other people online, they represent the same dangers as public chat rooms.

They may be taken for personal use during leisure time on the school's Y6 residential, providing it is made clear to children that they must not connect to the internet and play online with others, and that the child agrees to abide by this rule.

Procedures for using portable media players (e.g. iPads \ Android tablets):

Children are not allowed to bring their own portable media players into school. However, children are allowed to take these items with them on the Y6 residential for the sole purpose of listening to music.
Staff may use their portable media player in school in their own time (e.g. lunchtimes).

Sanctions to be imposed if procedures are not followed:

If rules are broken and procedures are not adhered to by individual children:

- Letters may be sent home to parents or carers (if applicable).
- Users may be suspended from using the school's computers, Internet or Google system etc. for a given period of time.
- Details may be passed on to the police in more serious cases.
- Legal action may be taken in extreme circumstances.

Cases of misuse will be considered on an individual basis by the Headteacher, Deputy Headteacher, Computing co-ordinator or class teacher (depending on their seriousness) and sanctions agreed and imposed to 'fit the crime.'

Responding to concerns about the safety of children:

When there are concerns about the welfare of a child arising from the use of electronic media then the school will use its usual safeguarding children's procedures and good practice to respond to these. In this sense the context of electronic media is no different to other situations where there is a concern about a child's welfare.

If there is a concern about actual significant harm or the risk of significant harm to a child or young person arising from the use of electronic media then the school will immediately activate its own safeguarding children or child protection procedures, use the *TSCB Safeguarding Children Framework* and make a referral to the Multi Agency Safeguarding Hub (MASH). Again, this is no different to concerns in other situations. If a child is in immediate danger, then the school will contact the Police.

Responding to concerns about the use of electronic media by staff and volunteers:

If staff (paid/unpaid) use electronic media in ways that cause concern, then this will be dealt with under the auspices of the acceptable use policy or procedure of the school.

However, if that use by staff or volunteers amounts to a concern about an abusive relationship with, or harmful behaviour towards, a child or then the Tameside Safeguarding Children Framework procedures should be activated. Specifically, steps should be taken by the school as set out in the TSCB *Management of Allegations against Staff* procedure. This will include consultation with the school's designated senior manager in respect of allegations (the Headteacher) and subsequently with the Local Authority Designated Officer (LADO).

Equality

This policy is linked to our Equality Policy.

We aim to:

- Eliminate unlawful discrimination, harassment, victimisation and other conduct prohibited by the Equality Act 2010.
- Advance equality of opportunity between people who share a protected characteristic and people who do not share it.
- Foster good relations across all characteristics – between people who share a protected characteristic and people who do not.

At Aldwyn Primary school we will continuously strive to ensure that everyone is treated with respect and dignity. Each person will be given fair and equal opportunities to develop their full potential regardless of:

- Age
- Disability
- Gender reassignment
- Marriage or civil partnership
- Pregnancy or maternity
- Race
- Religion or belief – including lack of belief
- Sex
- Sexual orientation

Safeguarding

At Aldwyn Primary School, the welfare and safety of our children is our paramount concern. We will promote the health, well-being and safety of the pupils in all we do. All our children have the right to protection, regardless of age, gender, race, culture or disability. They have a right to be safe in our school. We take seriously our duty to safeguard and promote the welfare of the children in our care.

Safeguarding children is everyone's responsibility.

Concluding Statement

The procedures in this policy will be subject to ongoing review and modification in order to keep up with advances in the technology coming into the school and that this policy will not remain static.

It may be that staff or children might wish to use an emerging technology for which there are currently no procedures in place. The use of any emerging technologies will be permitted upon completion and approval of a risk assessment, which will be used to inform future policy updates. Risk assessments will be approved by the Health & Safety Manager (the Head Teacher).

Appendix

i. **Acceptable Use Agreement (AUP) for Staff**

ii. **12 Rules for Responsible Computer Use**

iii. **E-safety home/school agreement**

Appendix i

Acceptable Usage Policy
(Staff)

1. I will not divulge any school related passwords and I will comply with school IT security procedures.
2. I will make sure email and social media interactions with staff, parents, pupils and members of the public are responsible and in line with school policies and DfE/GTC/TA guidelines.
3. I will only use school IT systems, external logins and email for school related purposes. Other use will be with the permission of a SLT teacher.
4. I will not give my home address, phone number, mobile number, personal social networking details or email address to pupils. I accept that pupils may find these details out, and that any contact should be logged and either not reciprocated or replied to in line with school policies. I should be responsible and aware of my professional responsibilities and school policies if I supply any personal details to parents.
5. I will use school email systems for school related communications. I will not use personal accounts for school business.
6. I will ensure that personal data is stored securely and in line with the Data Protection Act. I will follow school policy with regard to external logins, encrypted data and not storing school material on personal IT equipment.
7. I will not install software onto workstations or the network unless supervised by the network manager or IT support staff.
8. I will not search for, view, download, upload or transmit any material which could be considered illegal, offensive, defamatory or copyright infringing.
9. Photographs of staff, pupils and any other members of the school community will not be used outside of the internal school IT network unless written permission has been granted by the subject of the photograph or their parent/guardian. I will ask the Headteacher (on site) or the proprietor of the building (off site) prior to taking any photographs.
10. I am aware that all network and internet activity is logged and monitored and that the logs are available to SLT in the event of allegations of misconduct.
11. I will not write or upload any defamatory, objectionable, copyright infringing or private material, including images and videos, of pupils, parents or staff on social media or websites in anyway which might bring the school into disrepute.
12. I will make sure that my internet presence does not bring the teaching profession into disrepute and that I behave online in line with DfE, GTC and TA guidelines.
13. I will champion the school's E-Safety policy and be a role model for positive and responsible behaviour on the school network and the internet.

Signed: ____

Dated: ____

Aldwyn Primary School

10 Rules for Responsible Computer Use.

Keeping safe: stop and think, before you click!

These rules will keep everyone safe and help us to be fair to everyone:

- I will only use the school's computers for schoolwork and homework.
- I will only delete my own files.
- I will not look at other people's files without their permission.
- I will ask permission from a member for staff before using the Internet.
- The messages I send, or information I upload, will always be polite and sensible.
- I will not open an attachment, or download a file, unless I have permission.
- I will not give out personal information – such as my name, address, phone number, or e-mail – or send photographs or videos to people I don't know and trust.
- I will not arrange to meet someone I have only been in touch with online, unless I have my parent's or carer's permission and they can be present.
- I will keep all my login and password details secret.
- If I see anything I am unhappy with or receive a message I do not like, I will not respond to it but I will tell a teacher/ responsible adult.

Child's name: ________________________________

Signature: ________________________________

Appendix iii

Aldwyn Primary School

E-safety home/school agreement

Parent/ Guardian name: ________________________________

Pupil name:____

E-safety agreement: As the parent or carer of the above pupil, I grant my permission for my child to have access to use of the Internet, school approved e-mail account and other ICT facilities at school.

I know that my child has signed an e-safety agreement form and that they have a copy of the '10 Rules for Responsible Computer Use'.

I accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the Internet and mobile technologies, but I understand that the school will take every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials. These steps include using an educationally filtered service, restricted access e-mail, employing appropriate teaching practice and teaching e-safety skills to pupils.

I understand that the school can check my child's computer files, and the Internet sites they visit and that if they have concerns about their e-safety or e-behaviour that they will contact me.

I will support the school by promoting safe use of the Internet and digital technology at home and will inform the school if I have any concerns over my child's e-safety.

I understand that I am permitted to take photographs/recordings of my child(ren) during school productions (e.g. assemblies) provided it is for my own use. Photos/videos taken that also include other children/members of staff MUST NOT be shared on social media.

Parent/ guardian signature: ______________________________________

Date: ________________________________

Please sign and return this copy of the agreement to your child's class.