



Annie Lennard Primary School

ONLINE SAFETY POLICY 2020-2021

REVIEW DATE: JUNE 2021

Rationale

The outside world is it 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 the internet and games consoles which is not age appropriate. It is essential to address this and to encourage a lifestyle which incorporates a healthy balance of time spent using technology.

This policy also works in conjunction with the Acceptable Use Policy to protect the interests and safety of the whole school community and aims to provide clear advice and guidance on how to minimise risks and how to deal with any infringements. It is linked to the following school policies: child protection, health and safety, social media and networking, extremism, anti-bullying, mobile phone and data protection. The policy will also work in conjunction with the data protection act, GDPR and Keeping Children Safe in Education.

Both this policy and the Acceptable Use Policies (for all staff, governors, visitors and pupils) are inclusive of both fixed and mobile internet, technologies provided by the school (such as PCs, laptops, whiteboards, voting systems, digital video equipment, etc) and technologies owned by pupils or staff.

The technologies

ICT in the 21st Century has an all-encompassing role within the lives of children and adults. New technologies are enhancing communication and the sharing of information. Current and emerging technologies used in school and, more importantly in many cases, used outside of school by children include:

- ✓ The Internet
- ✓ e-mail
- ✓ Instant messaging
- ✓ Blogs
- ✓ Social networking sites
- ✓ Chat Rooms
- ✓ Gaming Sites
- ✓ Text messaging and picture messaging
- ✓ Video calls
- ✓ Online communities via games consoles

Whole school approach to the safe use of ICT

Creating a safe ICT learning environment includes three main elements at this school:

1. An effective range of technological tools which are filtered and monitored;
2. Interlinking policies and procedures, with clear roles and responsibilities;
3. A comprehensive e-Safety education programme for pupils, staff and parents.

Staff Roles and Responsibilities:

Online Safety is recognised as an essential aspect of safeguarding for all within the school community. The Headteacher, with the support of governors, aims to embed safe practices into the culture of the school. The Headteacher ensures that the policy is implemented and compliance with the policy monitored. The Headteacher and other members of the senior management team are also responsible for the safeguarding of children within the school. They are trained in online safety issues and are aware of the potential for serious child protection/safeguarding issues that may arise. (See safeguarding policy)

The responsibility for Online Safety has been designated to a member of the senior leadership team. Our school Online Safety Co-ordinator is Mrs Crozier. Our Online Safety Coordinator ensures they keep up to date with any Online Safety issues and guidance through liaison with the local authority representatives and through organisations such as The Child Exploitation and Online Protection (CEOP) and 360 degree safe. They will also liaise with the school's technical support to ensure that any issues regarding inappropriate websites are resolved. The school's Online Safety Coordinator

ensures the Head, senior management, staff and governors are updated as necessary. They are also in charge of leading the school's Online Safety Committee.

All staff are encouraged to create a talking culture in order to address any online safety issues which may arise in classrooms on a daily basis. They are also required to teach a robust and progressive online safety curriculum to help ensure that pupils within the school are fully aware of the benefits and risks of modern technology they experience both inside and outside of school.

The school has also appointed an Online Safety Committee. The members of this committee contain children from a variety of year groups within KS2. The Online Safety Committee both represent and educate the teachers and children of Annie Lennard on the importance of staying safe online. Members also regularly discuss and share ideas on how we, as a school, can improve the teaching and awareness of online safety. The members of the committee are reappointed each year to allow for new voices and ideas to be added.

Our ICT is managed by Sandwell Local Authority. The ICT technician assigned to our school needs to ensure that the school's technical infrastructure is secure and is not open to misuse or malicious attack. They also need to ensure that users may only access the networks and devices through a properly enforced password protection policy. The technician ensures that the filtering policy is applied and updated on a regular basis.

All children within the school are responsible for using the school's ICT technology in accordance with the student/pupil acceptable use agreement. They also have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations. This is taught to them through our Online Safety curriculum. All children also understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.

Parents/guardians play a crucial role in ensuring that their children understand the need to use the internet or mobile devices in an appropriate way. Our school will take every opportunity to help parents understand these issues through parent workshops, newsletters, text alerts and updates to the Online Safety section of the website. Parents and carers will be encouraged to support the school/academy in promoting good online safety practice and to follow guidelines on the appropriate use of digital and video images taken at school events as well as access to parents' sections of any website provided by the school.

All visitors also receive our e-safety agreement on arrival at school and are expected to follow the policies outlined within this document.

Staff awareness

- ✓ All staff receive regular information and training on online safety issues in the form of in-house training and meeting time.
- ✓ All staff are required to read and sign the school's Acceptable Use Policy. New staff receive information on this as part of their induction.
- ✓ All staff are made aware 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.
- ✓ All staff are encouraged to incorporate online safety activities and awareness within their curriculum areas and through a culture of talking about issues as they arise.
- ✓ When incidents occur relating to online safety, Staff are required to report the incident via My Concern. If this is not possible then they will report directly to the school's designated safeguarding person, Mrs N Crozier. If this is not possible they report to either of the school's deputy safeguarding person, Mrs J Rogman or Mrs E Hadden
- ✓ All staff working with children are responsible for demonstrating, promoting and supporting safe behaviours in their classrooms and following school e-Safety procedures. These behaviours are summarised in the AUPs which must be signed and returned before use of technologies in school.

Internet:

- ✓ Annie Lennard School will use Broadband Sandwell (LGFL) “filtered” Internet Service, which will minimise the chances of pupils encountering undesirable material.
- ✓ Staff, pupils and visitors have access to the internet through the school’s fixed and mobile internet technology.
- ✓ Staff should email school-related information using their work email addresses and not through personal accounts.
- ✓ Staff will preview any websites before recommending to pupils to ensure it is relevant and suitable.
- ✓ Internet searches are conducted through Google, although the filtering system allows for any inappropriate sites or images to be blocked from the search.
- ✓ If staff or pupils discover an unsuitable site, the screen must be switched off immediately and the incident reported to the e-safety coordinator.
- ✓ If internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. All pupils have access to Curriculum Visions which provides information and texts that are safe and relevant for the children to complete their research.
- ✓ The CEOP Report Abuse button is available on the school website. Teachers make children aware of this and when it is appropriate to use it through their online safety curriculum and PSHE.
- ✓ Staff 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 not to deliberately seek out offensive materials. Should any pupils encounter any such material accidentally, they are expected to report it immediately to a teacher, so that the Service Provider (LGFL) can block further access to the site.
- ✓ Pupils are expected not to use any rude language in any online communications and contact only people they know or those the teacher has approved.
- ✓ They are taught the rules of etiquette in email and are expected to follow them.
- ✓ 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 summary of these ICT rules are to be displayed in all classrooms that have access to technology. Pupils will be asked to sign to this agreement, ensuring that they are aware of expectations. Copies of the agreement will also be distributed to parents to ensure that key messages are reinforced at home.
- ✓ The internet use agreement also appears when children log in to networked computers in school. They are required to click to agree to the policy before they are allowed to use the computers.

Passwords

Use a strong password (strong passwords are usually eight characters or more and contain 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 (laptops, iPads, netbooks, etc):

- ✓ Staff laptops should not be left in cars in conjunction with data protection and GDPR. If this is unavoidable, it should be temporarily locked out of sight in the boot.
- ✓ Staff should only use the laptop which is allocated to them.
- ✓ Mobile technology for pupil use, such as iPads and laptops, are stored in a locked trolley with the key stored separately to the trolley.
- ✓ Access is available via the school office keyholders.
- ✓ 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 only and are to be locked away in lockers (see mobile phone and cameras policy). If pupils bring in mobile phones (for the purpose of safety if they walk to and from school alone), they should be kept switched off. These are to be handed in where they are stored in a secure location throughout the school day (school Office). They are then handed back to the children

before they leave school. Any children not following these rules will be dealt with using the school's behaviour policy.

Data storage:

- ✓ All data is to be stored based on the Data Protection policy and GDPR.
- ✓ At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse
- ✓ Encrypt all removable media (USB pen drives, portable drives) taken outside school or sent by post or courier.
- ✓ Staff laptops should be encrypted if any data or passwords are stored on them.
- ✓ IPPs, assessment records, pupil medical information and any other data related to pupils or staff should not be stored on personal memory sticks.
- ✓ Any data sent by email to an outside party should be encrypted and the password should be sent separately.
- ✓ In the case of a possible breach, you must understand the need for urgency and know who to report it to within the school.
- ✓ Any access personal data sources and records only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- ✓ You must not transfer any school/academy personal data to personal devices except as in line with school policy.
- ✓ Staff documents that include data are to be stored on their school OneDrive system or the school network. Both of these are encrypted for protection.
- ✓ Only take offsite information you are authorised to and only when it is necessary and required in order to fulfil your role.

Social Networking Sites:

Use such sites with extreme caution, being aware of the nature of what you are publishing on-line 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.

Your role in school requires a high degree of professionalism and confidentiality.

You should ensure that no reference is made on social media with regards to pupils, parents or other members of the school community.

You should also not engage in online discussion on personal matters relating to members of the school community

Any security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information

Any school networking sites, such as twitter, are run by a designated member of staff and only relevant and professional content should be uploaded at all times. All information must be approved by the Headteacher before publishing. Any images of children on these sites can only be added with the permission of the child's/children's parent or guardian.

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/guardians have **not** given permission for their child's image to be used in school. An up to date list is kept in the school office and that child's class teacher. Please be aware that permissions may be different depending on the purpose the image has been taken for.
- ✓ When using children's images for any school activity, they should not be identified by their name.
- ✓ This section of the policy is related to the to the mobile phone and cameras policy.

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

Providing a comprehensive E-safety education to pupils and parents

All staff working with children must share a collective responsibility to provide an online safety education to pupils and to promote online safety in their own actions.

Formally, an online safety education is provided by the objectives contained in the ICT unit plans for every area of work for each year group. Each year group will be required to follow the statement set out in the **Education for a Connected World** documentation. This will ensure that even if online safety is not relevant to the area of ICT being taught, it will still be a 'constant' in the ICT curriculum. Informally, a talking culture is encouraged in classrooms which allows online safety issues to be addressed as and when they arise.

The ICT Coordinator and the Online Safety Committee will lead assemblies throughout the year, including on Safer Internet Day, highlighting relevant online safety issues and promoting safe use of technologies.

All classes will follow a themed week at least once per year, during which their class teacher will lead lessons and activities designed to educate children in keeping safe when using the internet and other new technologies. Parents are also invited along to this event to help raise their awareness of current Online Safety issues.

All staff will ensure children know to report abuse using the CEOP button widely available on many websites or to speak to any member of staff, who will escalate the concern to the DSP or Deputy DSP through My Concern.

When children use any technology provided within school, such as laptops or iPads, staff should make sure children are fully aware of the agreement they are making to follow the school's ICT guidelines. These will have been signed by each child at the start of the school year.

Parents/carers will be invited to attend Online Safety workshops throughout the year, including Internet Safety Day. They will also be encouraged to interact with the Online Safety display that is located in the entrance of the school by the school office. Children will also have the opportunity to educate parents through assemblies and classroom activities on an annual basis.

Reporting an issue

As with other areas of school, if a member of staff, a child or a parent / carer has a complaint or concern relating to online safety then they will be considered and prompt action will be taken. Complaints should be addressed to the head teacher in the first instance, who will undertake an immediate investigation and liaise with the leadership team and those members directly involved. Incidents of e-safety concern will be reported and recorded via My Concern and reported to the school's designated safeguarding officer, Mrs N Crozier, in accordance with school's child protection policy. Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy.

Updating the Policy:

This policy will be reviewed and updated annually