WILLOW BROOK PRIMARY

E-Safety Policy

Date: September 2023
Next Review: September 2024

A member of the Griffin Schools Trust

E-Safety Co-ordinators – Allen Tsui and Gabrielle Ezekiel
Computing Co-ordinator – Allen Tsui
Safeguarding Lead – Mari Chivers

New technologies inspire children to be creative, communicate and learn. However, while the internet is a great resource, it is important that children and young people are protected from the risks they may encounter.

Willow Brook Primary School endeavours to highlight benefits and risks of using technology and provides Safeguarding and education for users to enable them to control their online experience. We believe that the key to developing safe and responsible behaviours online, not only for pupils but everyone within our school community, lies in effective education. We know that the internet and other technologies are embedded in our pupils' lives, not just in our school but outside as well, and we believe we have a duty to help prepare our pupils to safely benefit from the opportunities the internet brings.

- We will provide a curriculum, which has e-Safety related lessons embedded throughout.
- We will celebrate and promote e-Safety through a planned programme of assemblies and whole-school activities, including promoting Safer Internet Day each year.
- We will discuss, remind or raise relevant e-Safety messages with pupils routinely wherever suitable opportunities arise during all lessons; including the need to protect personal information, consider the consequences their actions may have on others, the need to check the accuracy and validity of information they use and the need to respect and acknowledge ownership of digital materials.
- Any internet use will be carefully planned to ensure that it is age appropriate and supports the learning objective for specific curriculum areas.
- Pupils well be taught how to use a range of age-appropriate online tools in a safe and effective way.
- School will model safe and responsible behaviour in their own use of technology during lessons.
- We will teach pupils how to search for information and to evaluate the content of websites for accuracy when using them in any curriculum area.
- When searching the internet for information, pupils will be guided to use age appropriate search engines. All use will be monitored and pupils will be reminded of what to do if they come across unsuitable content.
- Pupils will be taught about the impact of online bullying and know how to seek help if they are affected by any form of online bullying.
- Pupils will be made aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent or carer, teacher or trusted staff member, or an organisation such as Childline and CEOP (Child Exploitation and Online Protection).

Remote/Home Learning

- We will endeavour to ensure that pupils continue to receive a good level of education 'beyond the classroom' by providing a range of resources via our website (http://www.willowbrook-gst.org/) and learning portals, such as Purple Mash.
- We expect pupils to follow the same e-safety principles, as outlined in this policy, whilst learning at home.
- If our school chooses to communication with pupils over the coming weeks/months via Zoom, Teams, Skype etc. then it is important that this be only carried out with the

approval of the Head or Senior Leader. Pupils must uphold the same level of behavioural expectations, as they would in a normal classroom setting.

- Any significant behavioural issues occurring on any virtual platform must be recorded, reported and appropriate sanction imposed. For all minor behavioural incidents, these should be addressed using the normal restorative approaches.
- Staff should be mindful that when dealing with any behavioural incidents, online, opportunities to discuss and repair harm would not be the same as if the child or young person was in school. Therefore, it may be necessary to have a discussion with the parents, regardless how minor the incident, to ensure the child is emotionally well supported.
- All parents will be required to sign the home-school agreement.

Zoom Home-School Agreement

Parents and pupils must adhere to the following steps at all times:

1. Sign in with your child's first name only (not their surname or any middle names).
2. Mute your microphone before joining the meeting and keep it muted unless asked to unmute.
3. Avoid using the chat facility for anything other than questions associated with learning (Remember you can use 2email to communicate directly with your class teacher).
4. Be respectful to all participants.
5. Dress in appropriate clothing.
6. Avoid eating whilst participating in the Zoom sessions.
7. Ensure you are in an appropriate room in your house (e.g. somewhere that you can concentrate).
8. Ensure the background positioned is appropriate - download one of the Zoom default backgrounds if necessary.
9. Where possible, support your child to participate in the session and complete the activities set.
10. Uphold our normal behaviour expectations.
11. Only the teacher is permitted to record the session.

By joining a Zoom meeting organised by Willow Brook Primary, you agree to follow the expectations stated above.

General Note for incident in school or online

At every stage the child should be involved in or informed of the action taken. Urgent or serious incidents should be referred straight to the head teacher, or a member of SLT. If necessary, refer to the other related internal policies. Normal recording systems on EDUKEY should continue, entries should be factual and action/follow up recorded also.

Staff Training

Our staff receive regular information and training on e-Safety issues, as well as updates as and when new issues arise. All staff will be made aware of individual responsibilities relating to the safeguarding of children within the context of e-safety and know what to do in the event of misuse of technology by any member of the school community. All staff will be encouraged to incorporate e-Safety activities and awareness within their curriculum areas.

Managing ICT Systems and Access

The school will agree on which users should and should not have internet access and the appropriate level of access and supervision they should receive. Users will be made aware that they must take responsibility for their use and behaviour while using the school ICT system and that such activity will be monitored and checked. All internet access will be undertaken alongside a member of staff or, if working independently, a member of staff will supervise at all times. Members of staff will access the internet using an individual ID and password, which they will keep secure. They will ensure that they log out after each session and not allow pupils to access the internet through their ID or password.

Managing Filtering

- The school will work with relevant providers to ensure systems which protect pupils are regularly reviewed and improved.
- If staff or pupils discover an unsuitable site, it must be reported to the E-Safety Leader. Concerns are escalated to the Technical service provider where necessary.
- If users discover a website with potentially illegal content, this should be reported immediately to the e-Safety Co-ordinator. The school will report such incidents to appropriate agencies including Internet Service Provider (ISP), Police, CEOP or the Internet Watch Foundation (IWF).
- Any amendments to the school filtering policy or block and allow lists will be checked and assessed by the Senior Leadership Team /e-Safety Co-ordinator prior to being released or blocked.
- The evaluation of online content materials is a part of teaching and learning in every subject and will be viewed as a whole-school requirement across the curriculum.

E-Mail

- Staff and pupils should only use approved email accounts allocated to them by the school and should be aware that any use of the school email system will be monitored and checked.
- Staff should not use personal email accounts for professional purposes, especially to exchange any school related information or documents or to email parents/carers.
- Irrespectively of how pupils or staff access their school email (from home or within school), school policies still apply.

Social Networking

- Staff will not post content or participate in any conversations which will be detrimental to the image of the school. Staff who hold an account should not have parents or pupils as their 'friends'. Doing so will result in disciplinary action or dismissal.
- School blogs or social media sites should be password protected and run from the school website with approval from the Senior Leadership Team.
- Pupils and parents are advised that the use of some social network spaces, for example Facebook, Instagram and TikTok, is inappropriate for primary aged pupils and that some of these sites have minimum age requirements.

Pupils Publishing Content Online

- Pupils will not be allowed to post or create content on sites unless the site has been approved by a member of the teaching staff.
- Pupils' full names will not be used anywhere on the website, particularly in association with photographs and video.
- Written permission is obtained from the parents/carers before photographs and videos are published.
- Any images, videos or sound clips of pupils must be stored on the school network and never transferred to personally-owned equipment.
- Pupils and staff are not permitted to use portable devices to store images/video/sound clips of pupils. Mobile Phones and Devices General use of personal devices
- In the case of school productions, Parents/carers are permitted to take pictures of their child in accordance with school protocols which strongly advise against the publication of such photographs on social networking sites.
- The sending of abusive or inappropriate text, picture or video message is forbidden.

Pupils' use of personal devices

- Pupils' who need to bring a mobile phone in to school can do so, however phones will be handed in to teachers at the start of the day and stored appropriately.
- Pupils who do not follow the school policy relating to the use of mobile phones will not be permitted to bring their mobile phones into school.

CCTV

- The school may use CCTV in some areas of school property as a security measure.
- Cameras will only be used in appropriate areas.

General Data Protection

General Data Data Protection (GDPR) and e-safety Data must always be processed lawfully, fairly and transparently; collected for specific, explicit and legitimate purposes; limited to what is necessary for the purposes for which it is processed; accurate and kept up to date; held securely; only retained for as long as is necessary for the reasons it was collected. GDPR is relevant to e-safety since it impacts on the way in which personal information should be secured on school networks, computers and storage devices; and the security required for accessing, in order to prevent unauthorised access and dissemination of personal material. Staff need to ensure that care is taken to ensure the safety and security of personal data regarding all of the school population and external stakeholders, particularly, but not exclusively: pupils, parents, staff and external agencies. Personal data should only be stored on secure devices.

Support for Parents

- Parents attention will be drawn to the school's e-Safety policy and safety advice in newsletters, the school website and e-Safety information workshops.
- The school website will be used to provide parents with timely and meaningful information about their children's school lives and work to support the raising of achievement. The website will also provide links to appropriate online-safety websites.

Radicalisation Procedures and Monitoring

It is important for us to be constantly vigilant and remain fully informed about the issues which affect the region in which we teach. Staff are reminded to suspend any professional disbelief that instances of radicalisation 'could not happen here' and to refer any concerns through the appropriate channels (currently via the Child Protection/Safeguarding Coordinator). Regular monitoring and filtering is in place to ensure that access to appropriate material on the internet and key word reporting it in place to ensure safety for all staff and pupils.

Sexual Harassment

Sexual harassment is likely to: violate a child's dignity, make them feel intimidated, degraded or humiliated and/or create a hostile, offensive or sexualised environment. Online sexual harassment, which might include non-consensual sharing of sexual images and videos and sharing sexual images and videos (both often referred to as 'sexting'; inappropriate sexual comments on social media; exploitation; coercion and threats). Any reports of online sexual harassment will be taken seriously, and the police and Children's Social Care may be notified. Our school follows and adheres to the national guidance - UKCCIS: *Sexting in schools and colleges: Responding to incidents and safeguarding young people.*

Responses to Incident of Concern

An important element of e-Safety is the ability to identify and deal with incidents of concern including the confidentiality of information. All staff, volunteers and pupils have a responsibility to report e-Safety incidents or concerns so that they may be dealt with effectively and in a timely manner in order to minimise any impact. The school has incident reporting procedures in place and record incidents of an e-Safety nature on Edukey. Misuse of the Internet may result in disciplinary action, including written warnings, withdrawal of access privileges, and in extreme cases, suspension or expulsion, in accordance with the relevant policies. The school also reserves the right to report any illegal activities to the appropriate authorities.