Crosby Primary School

Online Safeguarding Policy

Last reviewed Autumn 2024

Next Review Autumn 2025

This policy should be read in conjunction with the following policies:

- Child Protection and Safeguarding
- Staff Code of Conduct
- Data Protection
- Acceptable Use of IT

The Designated Safeguarding Lead is accountable for safeguarding provision (including online safeguarding) for all members of the school community. Online safeguarding is the responsibility of the whole-school community. **Any cause for concern should be reported to the Safeguarding Lead immediately.**

The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to the appropriate authorities.

Managing digital content

Written permission from parents or carers is obtained on entry to the school, regarding digital content, such as photographs of pupils being published on the school website or by an external body, e.g. 'X' (Twitter). Parents and carers can update their preferences by informing the school at any time. Staff and pupils only use school equipment to create and store digital images, video and sound. In exceptional circumstances, personal equipment may be used with permission from the Headteacher provided that any media is transferred solely to a school device and deleted from any personal devices.

Storage of Images

Any images, videos or sound clips of pupils must be stored on the school network and never transferred to personally-owned equipment. The school will store images of pupils that have left the school for up to 10 years following their departure for use in school activities and promotional resources. A selection of images may be retained for archive purposes. The IT Infrastructure Officer has the responsibility for deleting the images when they are no longer required.

Learning and Teaching

The key to developing safe and responsible behaviours online lies in effective education. We know that the internet and other technologies are embedded in our pupils' lives, not just in school but outside as well, and we believe we have a duty to help prepare our pupils to benefit safely from the opportunities the internet brings. We provide a series of specific online safety-related lessons in every year group as part of the computing and PSHE curriculum. We promote online safety through a planned programme of assemblies and whole-school activities, including promoting Safer Internet Day each year. We discuss, remind or raise relevant online 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.

Pupils are 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 or the CEOP 'report abuse' button.

Staff Training

Our staff receive regular information and training on online safety issues. 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 vigilant with regard to monitoring behaviour changes that may be as a result of new technology or online games being launched.

Social Media and Personal Publishing

Staff, volunteers, Governors, visitors and pupils should not breach confidentiality or bring Crosby Primary School into disrepute when posting on social media or personal publishing sites. Staff, volunteers, visitors, pupils and Governors must not share images or video of any school organised social events, including school performances, on social media sites. The school blocks access to social networking sites for pupil use within school, unless a specific use is approved. Staff will raise any concerns about pupil use of IT with parents/carers: this includes the use of any sites that are not age appropriate.

The School Website

The school website does not include the personal details, including individual email addresses or full names of pupils. A generic contact email address is used for all enquiries received through the school website. All content included on the school website must be approved by a senior member of staff before publication.

Managing IT Aystems and Access

The school is responsible for ensuring that access to the IT systems is as safe and secure as reasonably possible. Servers, workstations and other hardware and software are kept updated as appropriate. Virus protection is installed on all appropriate hardware, and is kept active and up to date. Users are made aware that they must take responsibility for their use and behaviour while using the school IT systems and that such activity could be monitored and checked. Members of staff only access information systems and the internet through individual ID and passwords. Staff must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence of a breach of security. Staff should change their passwords whenever there is any indication of possible system or password compromise. We recognise that it is good practice to change passwords on an annual basis. Staff should never save system-based passwords within an internet browser. Staff should create different passwords for different accounts and applications. Any cloud-based information system access containing school owned information assets will be managed by internal staff and approved contractors only.

Filtering Internet Access
The school uses a filtered internet service appropriate to the age and maturity of students. The filtering service produces reports of suspicious content for Headteacher review. If users discover a website with inappropriate or illegal content, this should be reported to a member of staff who will inform the Safeguarding Leader. The school will report such incidents to appropriate agencies. The evaluation of online content materials is a part of teaching and learning and is viewed as a whole-school requirement across the curriculum.

Email
School email accounts should be the only account that is used by staff for school-related business. For the safety and security of users and recipients, all mail is filtered and logged, and can be viewed by appropriate senior and technical staff. Staff and Governors are alerted to the dangers of opening email from an unknown sender or source; or viewing and opening attachments. All emails that are no longer required or of any value should be deleted.

Mobile Phones - Personal Use in School
All mobile phones carried by pupils must be handed in to a staff member if they are brought into school. If an inappropriate action is deemed to have taken place, the Headteacher has the right to confiscate the device and make further enquiries as appropriate.

Staff are not permitted to use their own mobile phones or devices for contacting children, young people or their families within or outside of the setting in a professional capacity. Mobile phones and personally-owned devices will be switched off whenever there are children present. However, in an emergency situation staff may use their own devices and hide (by inputting 141) their own mobile numbers for confidentiality purposes.

Data Protection and Information Security
Any access rights, including personal and sensitive information are reviewed regularly by the Headteacher

Management of Assets
Details of all school-owned and leased hardware is recorded in a hardware inventory. Details of all school-owned software is recorded in a software inventory. All redundant IT equipment is disposed of through an authorised agency at the discretion of the Headteacher. This includes a written receipt for the item including an acceptance of responsibility for the destruction of any personal data.

CCTV
There are visible signs showing that CCTV is in operation. Regular checks are carried out to ensure that the system is working properly and produces high quality images. CCTV footage may be used as evidence in relation to any Safeguarding or criminal activities that may occur on school premises.

Dealing with Complaints Published Online
All staff and Governors are aware of how to report any negative online comments about the school or members of the school community. Staff and Governors must under no circumstances reply or react to any online discussion about the school unless prior permission has been granted by the Headteacher. The complaints policy and procedure is clearly detailed on the school website.

Monitoring and Review

This policy is monitored and reviewed by the governing body. Last reviewed Autumn 2024.