Crosby School Primary School

Acceptable Use of Information Technology Policy

Reviewed Spring 2024

Next Review Spring 2025

Introduction

This policy describes the standards of acceptable use of Information Technology (IT) by children, staff, volunteers, visitors and governors. The policy also outlines the acceptable use of such technology by children and their parents/carers within school and whilst using school owned IT whilst at home. Whilst this policy covers a wide range of situations, it is recognised that it cannot cover every eventuality, however the principles contained within it must apply in every circumstance. It should be read in conjunction with other school policies, particularly:

- Child Protection and Safeguarding
- Data Protection
- Staff Code of Conduct

This policy adheres to KCSIE and all relevant updates.

We use the term IT to describe any kind of tool that you can use for sharing information, including but not limited to: blogs, photographs, videos, social networks, mobile phone applications, text, e-mail, digital TV services, wikis, and gaming and collaboration tools.

The use of IT for inappropriate purposes could constitute a criminal offence and breaches will be reported to the appropriate authorities.

Users are made aware through staff induction that they must take responsibility for their use and behaviour whilst using the school IT systems and that such activity could be monitored and checked. For the safety and security of users and recipients, all school email is filtered and logged, and can be viewed by appropriate senior and technical staff. Governors receive regular reports at the termly safeguarding meeting on the outcomes of monitoring.

Any access to personal and sensitive information should be assessed and granted by the headteacher in accordance with the Data Protection policy. Reference, in school access hierarchy.

Purpose

The purpose of this policy is to protect and promote the interests of adults and the children they work with. All adults have a legal and moral duty to keep children safe and to protect them from harm. **Any cause for concern must be reported to the Safeguarding Lead or the Deputy Safeguarding Lead immediately who will follow Safeguarding policies and may inform the police where appropriate.**

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 except the school website with the consent of the headteacher. 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.

Responsibilities

Responsibilities of Children

- Only use IT in school when told to by a member of staff
- Don’t bring mobile phones or other electronic devices into school. If you do, hand them in straight away. If the device gets lost or damaged this is your fault for bringing it into school
- Be polite when communicating electronically
- Tell an adult in school if you see or hear anything that you think is wrong
- If an inappropriate action may have taken place, the headteacher, with another member of staff present, has the right to confiscate and search the device in question to extract any potential evidence.

Responsibilities of Visitors/Contractors

- Turn off your mobile device while on school premises, unless you have specific consent from the Headteacher

Responsibilities of Parents/Carers

- Don't take photographs/videos/recordings at school events or on school premises unless you are told by the headteacher that you can.
- Don't damage the reputation of the school, its staff or pupils by what you put online.
- Share any concerns or complaints directly with the school by following the school's complaints procedure which is available via the school website.

Responsibilities of Staff, Volunteers and Governors

Safeguarding Children

- Mobile phones and personally-owned devices must not be used whenever there are children present except in exceptional circumstances.
- Do not use mobile phones to take images of children.
- Do not access, make or store indecent images of children on the internet, to do so would be illegal and lead to a criminal investigation.
- Any images, videos or sound clips of pupils must be stored on the school, Google Drive network or secure storage devices and never transferred to personally-owned equipment.
- Do not make, use or store images that may cause distress or offence.
- Have parental consent to distribute any images of children beyond the school community (e.g. website, press, etc.).
- Be clear about the purpose of any activity involving photography and what will happen to the images when the activity is concluded. Be able to justify the reason for having images of children in your possession.
- Do not take images of children in one to one situations.
- All content included on the school website must be approved by a senior member of staff before publication.
- Ensure children are supervised at all times when IT is being used by the children on the school site or off site during field visits. It is the responsibility of the person supervising the children engaged in IT to ensure they use the internet responsibly.
- Ensure that any materials shown to children are age appropriate and that children are not exposed to unsuitable material through IT.
- Our internet provider screens content but no system is foolproof. Any cases of children accidentally viewing unsuitable sites should be reported to the IT Support Assistant and the Safeguarding Lead immediately. This will then be reported to the internet provider to block access in the future.
- **If you have any safeguarding concerns you must immediately report them to the Safeguarding Lead or Deputy Safeguarding Lead.**

Data Security

- The personal data of others must be treated with care and respect. Keep private and sensitive information confidential at all times and only share it with relevant professionals when it is in the interests of the child to do so.
- The personal data of children and staff should not be taken off the premises if possible (for example laptops, non-encrypted mobile data storage devices, or unapproved clouds). If the personal data of children or staff must be taken off site for professional purposes, it must be encrypted whenever possible.
- Personal information about other people must not be placed on social media as this is their information and any such disclosure of personal information could be a breach of the law. The school can be held liable for your actions so if you are unsure about whether you are acting within the law you should seek legal clarification.
- Do not allow other users to access the systems using your log on details and must immediately report any suspicion or evidence of a breach of security. Passwords must be kept safe. Update your passwords regularly and do not share them.
- Change your password whenever there is any indication of possible system or password compromise. Staff should never save system-based passwords within an internet browser.

- Create different passwords for different accounts and applications. Passwords should reflect school guidance, eg. 3 random words**.** Any cloud-based information system access containing school owned information assets will be managed by internal staff and approved contractors only.
- Ensure that the protection settings are left as set up by the technician (e.g. that Windows Firewall always runs, passwords are in place).
- Ensure school equipment (e.g. laptops) is not used by unauthorised persons, including family and friends.
- Always lock your screen if you are away from your laptop.
- Laptops in cars must be stored out of sight (e.g. in covered boot). Laptops should never be left in a vehicle for prolonged periods of time or overnight.
- **If you are attacked, don't risk your own safety. Hand over the laptop. It can be replaced but you can't.**
- Unauthorised or unlicensed software must not be loaded on to the laptop.
- Take all reasonable steps to ensure that the laptop is not damaged through misuse.
- When travelling, laptops should not be left unattended in public places.
- Remain particularly vigilant when using your laptop and try to refrain from using it in public places (e.g. library, railway station). Personal data must not be accessed in a public place.
- Return the laptop to school for regular health checks or when requested and ensure that the laptop antivirus software is updated by the school IT technician.
- Back up your files regularly and store them securely.
- School email accounts must be the only account that is used by staff for school-related business. Be alert 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.
- Return the laptop before leaving the employment of the school.
- Report any possible security breaches (e.g. laptop stolen or misplaced) to the headteacher immediately.
- Staff receive regular updates/training regarding cyber security.

<u>Communication with Children and Parents/Carers</u>

- Use the school's approved text, email messaging service and X (formerly Twitter) to communicate with parents/carers.
- Only make contact with children for professional reasons and in accordance with organisational policy.
- Only use approved and secure internet or web-based communication channels to send messages including X (formerly Twitter). All emails accessed by children should be sent through ~~the DB learning platform.~~ Google Classroom Platform
- Only use personal text messaging as a last resort in an emergency when no other forms of communication are possible. However, in an emergency situation staff may use their own devices and hide (by inputting 141) their own mobile numbers for confidentiality purposes.
- Do not use your own mobile phones or devices for contacting children or their families in a professional capacity whether in school or off the premises. Only use equipment provided or authorised by the school.
- Do not request, or respond to any personal information from a child, ensuring that communication only takes place within clear and explicit professional boundaries through the school's own communication channels.
- Do not give your personal contact details to children, including your mobile number, home phone or personal email address, unless the need to do so is agreed with the headteacher and parents/carers.
- Any communication made by X (formerly Twitter) should be uploaded by IT Infrastructure Officer and/or the Support Assistant for IT and computing.

<u>Reputation of the School</u>

- You are personally responsible for your actions and anything you say online. Conduct that is likely to bring discredit to the school will be dealt with in accordance with the school's disciplinary procedure.
- It is your own choice whether or not you participate in any kind of social media activity in your own time. Whilst the views and opinions you express are your own, as an employee you are still a representative of the school and should be aware that any information that you post about the school cannot be entirely separate from your working life.

Employees that make personal use of social media outside of work are advised not to identify their employer or role in order to avoid any confusion as to whether they are speaking as an employee or individual.

- Be aware that what you say can be accessed around the world within seconds; it may be shared or re-published elsewhere and will continue to be available indefinitely. You should also be mindful that even if information is restricted to your 'friends'/'followers' it is in effect public as you cannot control what they do with any information you post.
- Remember that laws relating to defamation, copyright and data protection apply when using social media (other laws may also apply). You should not make statements about other people or companies that could harm their reputation, and you should be careful not to copy the work of another person or company as this could be a breach of copyright laws.
- Social media sites must not be used during teaching time or in sight of pupils without the prior permission of the headteacher.
- We recommend that profiles on social media sites are set and maintained to maximum privacy and to give access to known friends only.
- Report any incidents of cyberbullying to the headteacher-incidents will be dealt with in line with the school's Pupil Discipline policy.
- Be aware that participating online in a personal capacity may attract media interest in you as an individual, so proceed with care.
- Set the tone for online messages and conversation by being polite, open and respectful. Use familiar language and be cordial and professional at all times. You must ensure that you respect people's confidentiality and do not disclose non-public information or the personal information of others. If you are unsure what information is in the public domain then always seek clarification before divulging anything.
- Ensure accuracy of information; be fair, thorough and transparent. Never publish anything you are unsure about and be confident and clear in what you say.
- Wherever possible, align online participation with the school's website and other offline communications e.g. school newsletter.
- Report any negative online comments about the school or members of the school community. Under no circumstances reply or react to any online discussion about the school unless prior permission has been granted by the headteacher.
- Add a disclaimer to your blog or social media profile to make it clear that your accounts and views are personal, e.g. "these views are my own and do not necessarily represent the views of my employer", if you have identified the school as your employer.

Monitoring and Review
This policy is monitored and reviewed by the governing body. Last reviewed Spring 2024