Crosslee Community Primary School

E-safety Policy

June 2021

Contents

Aims

It is the duty of the School to ensure that every child and young person in its care is safe. Safeguarding and promoting the welfare of pupils is embedded into the culture of the school and its everyday practice and procedures. All staff have a responsibility to support e-Safe

practices in school and all pupils need to understand their responsibilities in the event of deliberate attempts to breach e-safety protocols.

This policy applies to all members of the school community including: staff, pupils, volunteers, parents/carers, visitors and community users who have access to and are users of school IT systems, both in and out of the school.

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and education the whole school community in its use of technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

Legislation and guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education 2021 (updated Jan), and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying
- Relationships and sex education
- Searching, screening and confiscation

The Education and Inspections Act 2006 empowers Head teachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other e-safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data where schools believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

Roles and Responsibilities

The following section outlines the e-safety roles and responsibilities of individuals and groups within the school:

Governors:

Governors are responsible for monitoring this policy, the approval of the E-Safety Policy and for reviewing the effectiveness of the policy and holding the Head teacher to account for its implementation. This will be carried out by receiving regular information about e-safety incidents and monitoring reports. The governor who oversees the online safety is the safeguarding lead governor Sue Nicholson.

Head teacher (Mrs Wadsworth):

- The Head teacher has a duty of care for ensuring the safety (including e-safety) of members of the school community.
- The Head teacher is responsible for ensuring the staff understand this policy, and that it is being implemented consistently throughout the school.
- The Head teacher and safeguarding leads aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.
- The Head teacher is responsible for ensuring that the e-safety co-ordinator (Miss Crew) receives suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.
- The Head teacher will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.

The designated safeguarding lead (Miss Crew):

Details of the school's DSL are set out in the Crosslee Community Primary School Safeguarding Policy.
The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the Head teacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- takes day-to-day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policy.
- provides training and advice for staff.
- liaises with the relevant bodies e.g. CEOP, Manchester Local Authority.
- liaises with school network technician.
- Ensuring that any online safety or cyber-bullying incidents are logged and dealt with appropriately in line with the Crosslee Community Primary School Behaviour and Anti-Bullying Policy.

All staff and volunteers:

All staff, including contractors and agency staff, and volunteers are responsible for:

- they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices;
- they have read, understood and signed the Staff Acceptable Use Policy.
- Implementing this policy consistently.
- they report any suspected misuse or problem to the DSL (Miss Crew) for investigation and appropriate action.
- all digital communications with students / pupils / parents / carers should be on a professional level and only carried out using official school systems;
- e-safety issues are embedded in all aspects of the curriculum and other activities;
- the children understand and follow the e-safety and acceptable use policies;
- the children have a good understanding of research skills and uphold copyright regulations;
- they monitor the use of digital technologies, mobile devices, iPads, cameras etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices;
- in lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

Pupils:

- are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Policy;
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations;
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so;
- they should know and understand what cyber-bullying means;
- should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school.

Parents / Carers

Parents / Carers play the primary role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters and information about national / local e-safety campaigns / literature. Parents and

carers will be encouraged to support the school in promoting good e-safety practice and to follow guidelines on the appropriate use of:

- Digital and video images taken at school events
- Access to social media, parents' sections of the website and school endorsed on-line activity that may contain recorded pupil data.

Parents/ Carers are expected to:

- Notify a member of staff of the DSL (Miss Crew) of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms of the school's acceptable use policy.

Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and are expected to read and follow it. If appropriate, they will be expected to agree to the terms of the school's acceptable use policy.

Technical

Staff

MGL ICT Support Technician (L Sachor) are responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets required e-safety technical requirements and any Local Authority guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed.
- blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- that they keep up to date with e-safety technical information in order to effectively carry out their e-safety roles and to inform and update others as relevant.
- that the use of the network / internet / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Head teacher for investigation.
- that monitoring software / systems are implemented and updated as agreed in school policies.

Infrastructure / equipment, filtering and monitoring

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities:

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements.
- There will be regular reviews and audits of the safety and security of technical systems.
- Servers, wireless systems and cabling must be securely located and physical access restricted.
- All users will have clearly defined access rights to school technical systems and devices.
- Software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations. Inadequate licencing could cause the school to breach the Copyright Act which could result in fines or unexpected licensing costs.
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by MGL. Content lists are regularly updated and internet use is regularly monitored. There is a clear process in place to deal with requests for filtering changes.
- The school has provided enhanced user-level filtering.
- School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.
- An appropriate system is in place for users to report any actual / potential technical incident / security breach to the relevant person (Mrs Crew, Miss Allison, Mr Sachor), as agreed.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- Procedures are in place for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the school systems.
- An agreed policy is in place regarding the extent of personal use that users (staff / pupils / community users) and their family members are allowed on school devices that may be used out of school.
- An agreed policy is in place that allows staff to download executable files and install programmes on school devices.
- An agreed policy is in place regarding the use of removable media (e.g. memory sticks / CDs / DVDs) by users on school devices. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to

learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet.

Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular, they should recognise the risks attached to publishing their own images on the internet (e.g. on social networking sites).
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other pupils in the digital / video images.
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs, unless express parental permission has been sought beforehand.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website (covered as part of the data protection privacy notice signed by parents or carers at the start of the year).

Data Protection

In accordance with the requirements outlined in the Data Protection Act 2018, personal data will be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals.
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical

purposes shall not be considered to be incompatible with the initial purposes.
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- Accurate and, where necessary, kept up-to-date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods, insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by the Data Protection Act 2018 in order to safeguard the rights and freedoms of individuals.
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. When using communication technologies, the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. An encrypted email service for the sharing of personal information outside of the school system is available to staff.
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and pupils or parents / carers (email, chat, etc.) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Pupils should be taught about e-safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff

Education pupils about online safety

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in e-safety is therefore, an essential part of the school's e-safety provision. The Computing Subject Lead is Miss Allison.

Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience. E-safety is a focus of the curriculum. The e-safety curriculum is broad, relevant and provides progression, with opportunities for creative activities and is provided in the following ways:

- A planned e-safety curriculum is provided as part of Computing / PHSE / other lessons and is regularly revisited.
- Key e-safety messages are reinforced as part of a planned programme of assemblies and whole school events, such as Safer Internet Day.
- Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Pupils should be helped to understand the need for the pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school
- Staff should act as good role models in their use of digital technologies the internet and mobile devices
- In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit. Children are also taught how to search for information that is relevant and appropriate for their age group.

In Key Stage 1, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies.

In Key Stage 2, pupils will be taught to:

- Use technology safely, respectfully
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns and content and contact.

By the end of primary school, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the important of respect for others online including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risk associated with people they have never met
- How information and data is shared and used online
- How to respond safely and appropriately to adults they may encounter whom they do not know

Educating parents/carers about online safety

Parents and carers may have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring of the children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond. The school will therefore seek to provide information and awareness to parents and carers through:

- Appropriate information web sites (e.g. www.thinkyouknow.co.uk)
- Information evenings / high profile events / campaigns e.g. Safer Internet Day

If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance the Head teacher (Mrs Wadsworth) or the DSL (Miss Crew).

Cyber-bullying

Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. E-safety is a partnership concern and is not limited to school premises and equipment or the school day. Bullying, harassment or abuse of any kind via digital technologies or mobile phones will not be tolerated and complaints of cyber bullying will be dealt with in accordance with the School's Behaviour and Anti-Bullying Policy.

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will discuss cyber-bullying with their tutor groups.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

Complaints related to child protection will be dealt with in accordance with the school's Safeguarding Policy.

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures.

Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm
- Disrupt teaching
- Break any of the school values

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material
- Retain it as evidence (of a criminal offence or a breach of school discipline)
- Report it to the police

Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation and the school's COVID-19 risk assessment.
Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

Prevent

In accordance with the Prevent Strategy, which aims to prevent children and young people being exposed to extremist views and at risk of radicalisation, staff are all trained on the Prevent Strategy.

This responsibility extends to online safety and protecting children from extremist material online. Through this training, staff are aware of how the internet is used to radicalise people. Filtering should prevent access to such extremist sites but any material accessed at school should be treated as an online safety incident and dealt with accordingly. Disclosures or concerns regarding exposure outside of school should be treated as a safeguarding incident and dealt with in accordance with the Safeguarding policy and procedures

Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.
More information is set out in Crosslee Community Primary School Acceptable Use Policy.

Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date – always install the latest updates

Staff members must not use the device in any way which would violate the Crosslee Community Primary School Acceptable Use Policy.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from MGL ICT Support Technician (L Sachor).

How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on anti-bullying and behaviour and acceptable use. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

Training

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal e-safety training is compulsory for all staff. This will be regularly updated and reinforced.
- All new staff will receive e-safety training as part of their induction programme, ensuring that they fully understand the school E-safety Policy and Acceptable Use Policy.

The DSL (Miss Crew) and deputy (Mrs Wadsworth) will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals.

Monitoring Arrangements

Behaviour and safeguarding issues relating to online safety are logged on CPOMs.

Issues relating to accessing inappropriate websites are reported to the Head teacher (Mrs Wadsworth) as they occur and/or weekly and are investigated by the DSL (Miss Crew) and recorded on an online safety log.

Links with other policies

This online safety policy is linked to our:

- Safeguarding policy
- Anti-bullying and behaviour policy
- Acceptable use policy
- Staff Code of Conduct
- Device loan agreement