Love to Learn

E- SAFETY POLICY

ADOPTED DATE: JANUARY 2019
REVIEW DATE: JANUARY 2020

Malcolm Sargent Primary School
Empingham Road
Stamford PE9 2SR

Engage & Inspire * Nurture & Growth * Pride & Joy

Statement of intent

At Malcolm Sargent Primary School (the school) we understand that computer technology is an essential resource for supporting teaching and learning. The internet, and other digital and information technologies, open up opportunities for pupils and play an important role in their everyday lives. Whilst the school recognises the importance of promoting the use of computer technology throughout the curriculum, we also understand the need for safe internet access and appropriate use. Our school has created this policy with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all pupils and staff. The school is committed to providing a safe learning and teaching environment for all pupils and staff, and has implemented important controls to prevent any harmful risks.

Signed by:

______________________ Headteacher Date: ______________________

______________________ Chair of governors Date: ______________________

1. Legal framework

1.1. This policy has due regard to the following legislation, including, but not limited to:

- Human Rights Act 1998
- Data Protection Act 1998
- Freedom of Information Act 2000
- Regulation of Investigatory Powers Act 2000
- Safeguarding Vulnerable Groups Act 2006
- Education and Inspections Act 2006
- Computer Misuse Act 1990, amended by the Police and Justice Act 2006
- Communications Act 2003
- Protection of Children Act 1978
- Protection from Harassment Act 1997
- General Data Protection Regulation (GDPR) May 2018

1.2. This policy also has regard to the following statutory guidance:

- DfE (2016) 'Keeping children safe in education'

1.3. This policy will be used in conjunction with the following school policies and procedures:

- Behaviour Management & Exclusions Policy
- Anti-Bullying Policy
- Data Protection Policy
- Safeguarding & Child Protection Policy
- Allegations of Abuse Against Staff Policy
- Staff Acceptable Use Policy & Agreement
- Pupils' Acceptable Use Policy & Agreement
- PSHE Policy
- Teaching & Learning Policy

2. Use of the internet

2.1. The school understands that using the internet is important when raising educational standards, promoting pupil achievement and enhancing teaching and learning.

2.2. Internet use is embedded in the statutory curriculum and is therefore an entitlement for all pupils, though there are a number of controls the school is required to implement to minimise harmful risks.

2.3. When accessing the internet, individuals are especially vulnerable to a number of risks which may be physically and emotionally harmful, including:

Access to illegal, harmful or inappropriate images
Cyber bullying
Access to, or loss of, personal information
Access to unsuitable online videos or games
Loss of personal images
Inappropriate communication with others
Illegal downloading of files
Exposure to explicit or harmful content, e.g. involving radicalisation
Plagiarism and copyright infringement
Sharing the personal information of others without the individual's consent or knowledge

3. Roles and responsibilities

3.1. It is the responsibility of all staff to be alert to possible harm to pupils or staff due to inappropriate internet access or use, both inside and outside of the school, and to deal with incidents of such as a priority.

3.2. The governing body is responsible for ensuring that there are appropriate filtering and monitoring systems in place to safeguard pupils. The governing body will appoint an e-safety governor to monitor this on its behalf.

3.3. The e-safety officer, Tim Cox, is responsible for ensuring the day-to-day e-safety in the school, and managing any issues that may arise.

3.4. The e-safety officer is responsible for chairing the e-safety committee, which includes representatives of the school senior leadership team (SLT), teaching staff, governors, parents and pupils.

3.5. The Data Protection Officer is responsible for ensuring the safeguarding of sensitive data and information regarding internet use and concerns flagged.

3.6. The Principal is responsible for ensuring that the e-safety officer and any other relevant staff receive CPD to allow them to fulfil their role and train other members of staff.

3.7. The e-safety officer will provide all relevant training and advice for members of staff as part of the requirement for staff to undergo regularly updated safeguarding training and be able to teach pupils about online safety.

3.8. The Principal will ensure there is a system in place which monitors and supports the e-safety officer, whose role is to carry out the monitoring of e-safety in the school, keeping in mind data protection requirements.

3.9. The e-safety officer will regularly monitor the provision of e-safety in the school and will provide feedback to the Principal.

3.10. The e-safety officer will maintain a log of submitted e-safety reports and incidents.

3.11. The Principal will establish a procedure for reporting incidents and inappropriate internet use, either by pupils or staff.

3.12. The e-safety officer will ensure that all members of staff are aware of the procedure when reporting e-safety incidents, and will keep a log of all incidents recorded.

3.13. Cyber bullying incidents will be reported in accordance with the school's Anti-Bullying Policy

3.14. The governing body will hold regular meetings with the e-safety officer to discuss the effectiveness of the e-safety provision, current issues, and to review incident logs, as part of the school's duty of care. The governing body will appoint an e-safety governor to manage this on its behalf

3.15. The governing body will evaluate and review this E-Safety Policy on an annual basis, taking into account the latest developments in ICT and the feedback from staff/pupils. The governing body will appoint an e-safety governor to manage this on its behalf

3.16. The Principal will review and amend this policy with the e-safety officer, taking into account new legislation, government guidance and previously reported incidents, to improve procedures.

3.17. Teachers are responsible for ensuring that e-safety issues are embedded in the curriculum and safe internet access is promoted at all times.

3.18. All staff are responsible for ensuring they are up-to-date with current e-safety issues, and this E-Safety Policy.

3.19. All staff and pupils will ensure they understand and adhere to our Acceptable Use Agreement, which they must sign and return to the Principal.

3.20. Parents are responsible for ensuring their child understands how to use computer technology and other digital devices appropriately.

3.21. The Principal is responsible for communicating with parents regularly and updating them on current e-safety issues and control measures.

3.22. All pupils are aware of their responsibilities regarding the use of school-based ICT systems and equipment, including their expected behaviour.

4. E-safety education

4.1. Educating pupils:

- An e-safety programme will be established and taught across the curriculum on a regular basis, ensuring that pupils are aware of the safe use of new technology both inside and outside of the school.
- Pupils will be taught about the importance of e-safety and are encouraged to be critically aware of the content they access online, including extremist material and the validity of website content.
- Pupils will be taught to acknowledge information they access online, in order to avoid copyright infringement and/or plagiarism.
- Clear guidance on the rules of internet use will be presented in appropriate places around the school.
- Pupils are instructed to report any suspicious use of the internet and digital devices.
- PSHE lessons will be used to educate pupils about cyber bullying, including how to report cyber bullying, the social effects of spending too much time online and where to access help.
- The school will hold e-safety events, such as Safer Internet Day and Anti Bullying Week, to promote online safety.

4.2. Educating staff:

- A planned calendar programme of e-safety training opportunities is available to all staff members, including whole school activities and CPD training courses.
- All staff will undergo e-safety training on an annual basis to ensure they are aware of current e-safety issues and any changes to the provision of e-safety, as well as current developments in social media and the internet as a whole.
- All staff will employ methods of good practice and act as role models for pupils when using the internet and other digital devices.
- All staff will be educated on which sites are deemed appropriate and inappropriate.
- All staff are reminded of the importance of acknowledging information they access online, in order to avoid copyright infringement and/or plagiarism.
- Any new staff are required to undergo e-safety training as part of their induction programme, ensuring they fully understand this E-Safety Policy.
- The e-safety officer will act as the first point of contact for staff requiring e-safety advice.

4.3. Educating parents:

- E-safety information will be directly delivered to parents through a variety of formats, including newsletters, the school website and social media.
- Twilight courses and presentations will be run by the school for parents.
- Parents' evenings, meetings and other similar occasions will be utilised to inform parents of any e-safety related concerns.

5. E-safety control measures

5.1. Internet access:

- Internet access will be authorised once parents and pupils have returned the signed consent form in Principal of all pupils who have been granted internet access.
- All users in key stage 2 and above will be provided with usernames and passwords, and are advised to keep these confidential to avoid any other pupils using their login details.
- Pupils' passwords will be changed on an annual basis and their activity is continuously monitored by the e-safety officer.

- Management systems will be in place to allow teachers and members of staff to control workstations and monitor pupils' activity.
- Effective filtering systems will be established to eradicate any potential risks to pupils through access to, or trying to access, certain websites which are harmful or use inappropriate material. These are provided by the internet service provider and managed by the school IT consultants Ark Ltd.
- Filtering systems will be used which are relevant to pupils' age ranges, their frequency of use of ICT systems, and the proportionality of costs compared to risks.
- The governing body will ensure that use of appropriate filters and monitoring systems does not lead to 'over blocking', such that there are unreasonable restrictions as to what pupils can be taught with regards to online teaching and safeguarding.
- Any requests by staff for websites to be added or removed from the filtering list must be first authorised by the e-safety officer.
- All school systems will be protected by up-to-date virus software.
- An agreed procedure will be in place for the provision of temporary users, e.g. volunteers.
- Master users' passwords will be available to the Principal for regular monitoring of activity.
- All internet use will only be monitored by the e-safety officer for access to any inappropriate or explicit sites, where it is justifiable to be necessary and in doing so, would outweigh the need for privacy.
- The school uses monitoring and safety software called Securus, which is updated regularly by Ark Ltd.
- Securus actively flags and informs the e-safety officer, any concerns or inappropriate activity, along with photographic evidence and details of user, time and date.
- Inappropriate internet access will be dealt with through the Disciplinary Policy.

5.2. Email:

- Pupils and staff will be given approved email accounts and are only able to use these accounts.
- The use of personal email accounts to send and receive personal data or information is prohibited.

- No sensitive personal data shall be sent to any other pupils, staff or third parties via email.
- Pupils are made aware that all email messages are monitored and that the filtering system will detect inappropriate links, viruses, malware and profanity.
- Staff members are aware that their email messages are monitored through the Securus software
- Any emails sent by pupils to external organisations will be overseen by their class teacher and must be authorised before sending.
- Chain letters, spam and all other emails from unknown sources will be deleted without opening.
- Staff ensure good practice regarding confidentiality to sensitive data and information by encrypting emails containing such content. This is done by typing the word 'encryptedemail' in the cc: box of the email they are sending. It ensures the email is password protected to be viewed by only the person in the 'send' list.

5.3. **Published content on the school website and images:**

- The Principal will be responsible for the overall content of the website, and will ensure the content is appropriate and accurate.
- Contact details on the school website will include the phone number, email and address of the school – no personal details of staff or pupils will be published.
- Images and full names of pupils, or any content that may easily identify a pupil, will be selected carefully, and will not be posted until authorisation from parents has been received.
- Pupils are not permitted to take or publish photos of others without permission from the individual.
- Staff are able to take pictures, though they must do so in accordance with school policies in terms of the sharing and distribution of such. Staff will not take pictures using their personal equipment.
- Any member of staff that is representing the school online, e.g. through blogging, must express neutral opinions and not disclose any confidential information regarding the school, or any information that may affect its reputability.
- The school will ask parent's permission for use of photos throughout the school, in the media and online, and will comply with these permissions.

5.4. Mobile devices and hand-held computers:

- The Principal may authorise the use of mobile devices by a pupil where it is seen to be for safety or precautionary use.
- Pupils are not permitted to access the school's Wi-Fi system at any times using their mobile devices and hand-held computers.
- Mobile devices are not permitted to be used during school hours by pupils or members of staff.
- Staff are permitted to use hand-held computers which have been provided by the school, though internet access will be monitored for any inappropriate use by the e-safety officer when using these on the school premises.
- The sending of inappropriate messages or images from mobile devices is prohibited.
- Mobile devices will not be used to take images or videos of pupils or staff.
- The school will be especially alert to instances of cyber bullying and will treat such instances as a matter of high priority.

5.5. Network security:

- Network profiles for each pupil and staff member are created, in which the individual must enter a username and personal password when accessing the ICT systems within the school.
- Passwords have a minimum and maximum length, to prevent 'easy' passwords or mistakes when creating passwords.
- Passwords will expire after 90 days to ensure maximum security for pupil and staff accounts.
- Passwords should be stored using non-reversible encryption.

5.6. Virus management:

- Technical security features, such as virus software, are kept up-to-date and managed by the IT Consultants for the school, Ark Ltd.
- The e-safety officer will ensure that the filtering of websites and downloads is up-to-date and monitored.

5.7. E-safety committee:

- The E-safety Policy will be monitored and evaluated by the school's e-safety committee on an annual basis.

- The committee will include a member of the SLT, the e-safety officer and the designated safeguarding lead (DSL), as well as members of the governing body, pupils and parents.

6. Social Media & Networking

- Teachers may not access social media during lesson time, unless it is part of a curriculum activity.
- Members of staff should avoid using social media in front of pupils.
- Members of staff **must not** "friend" or otherwise contact pupils or parents/carers through social media.
- If pupils or parents/carers attempt to "friend" or otherwise contact members of staff through social media, they should be reported to the Principal.
- Members of staff should avoid identifying themselves as an employee of the school on social media.
- Members of staff **must not** post content online which is damaging to the school or any of its staff or pupils.
- Where teachers or members of staff use social media in a personal capacity, they should make it clear that their views are personal.
- Teachers or members of staff must not post any information which could identify a pupil, class or the school.
- Members of staff should not post anonymously or under an alias to evade the guidance given in this policy.
- Breaches of this policy by members of staff will be taken seriously, and in the event of illegal, defamatory or discriminatory content, could lead to prosecution, disciplinary action or dismissal.
- Members of staff should be aware that if their out-of-work activity brings the school into disrepute, disciplinary action will be taken.
- Members of staff should regularly check their online presence for negative content via search engines.
- If inappropriate content is accessed online, the E-Safety Officer should be informed.
- Attempts to bully, coerce or manipulate members of the school community, via social media, by teachers and members of staff will be dealt with as a disciplinary matter.
- Members of staff should not leave a computer or other device logged in when away from their desk, or save passwords.
- Staff members should use their school email address for school business and personal email address for their private correspondence; the two should not be mixed.
- Pupils may not access social media during lesson time, unless it is part of a curriculum activity.

- Breaches of this policy by pupils will be taken seriously, and in the event of illegal, defamatory or discriminatory content could lead to prosecution, or exclusion.
- Members of staff should exercise caution and consider their professionality and professional boundaries at all times when using social media, and when profiles and comments they make online are visible to the wider school community.
- Pupils and parents/carers should not post anonymously or under an alias to evade the guidance given in this policy.
- Pupils and parents/carers **must not** post content online which is damaging to the school or any of its staff or pupils.
- Pupils must not sign up to social media sites that have an age restriction above the pupil's age.
- If inappropriate content is accessed online on school premises, it must be reported to a teacher.
- Access to social networking sites will be filtered as appropriate.
- Should access be needed to social networking sites for any reason, this will be monitored and controlled by staff at all times and must be first authorised by the Principal.
- Pupils are regularly educated on the implications of posting personal data online outside of the school.
- Staff are regularly educated on posting inappropriate photos or information online, which may potentially affect their position and the school as a whole.

7. Cyber bullying

7.1. For the purpose of this policy, cyber bullying is a form of bullying whereby an individual is the victim of harmful or offensive posting of information or images online.

7.2. The school recognises that both staff and pupils may experience cyber bullying and will commit to preventing any instances that should occur.

7.3. The school will regularly educate staff, pupils and parents on the importance of staying safe online, as well as being considerate to what they post online.

7.4. Pupils will be educated about online safety through teaching and learning opportunities as part of a broad and balanced curriculum; this includes covering relevant issues within PSHE lessons as well as sex and relationship education.

7.5. The school will commit to creating a learning and teaching environment which is free from harassment and bullying, ensuring the happiness of all members of staff and pupils.

7.6. The school has zero tolerance for cyber bullying, and any incidents will be treated with the upmost seriousness and will be dealt with in accordance with our Anti-Bullying Policy.

7.7. The Principal will decide whether it is appropriate to notify the police or anti-social behaviour coordinator in their LA of the action taken against a pupil.

8. Reporting misuse

8.1. Malcolm Sargent Primary School will clearly define what is classed as inappropriate behaviour in the Acceptable Use Agreement, ensuring all pupils and staff members are aware of what behaviour is expected of them.

8.2. Inappropriate activities are discussed and the reasoning behind prohibiting activities due to e-safety are explained to pupils as part of the curriculum in order to promote responsible internet use.

8.3. **Misuse by pupils:**

- Teachers have the power to discipline pupils who engage in misbehaviour with regards to internet use.
- Any instances of misuse should be immediately reported to a member of staff, who will then report this to the E-Safety Officer.
- Any pupil who does not adhere to the rules outlined in our Acceptable Use Agreement and is found to be wilfully misusing the internet, will have a letter sent to their parents explaining the reason for suspending their internet use.
- Members of staff may decide to issue other forms of disciplinary action to a pupil upon the misuse of the internet. This will be discussed with the Principal and will follow the schools Behaviour Management & Exclusions Policy.
- Complaints of a child protection nature, such as when a pupil is found to be accessing extremist material, shall be dealt with in accordance with our Safeguarding and Child Protection Policy.

8.4. **Misuse by staff:**

- Any misuse of the internet by a member of staff should be immediately reported to the Principal.

- The Principal will deal with such incidents in accordance with the Whistle Blowing Policy, and may decide to take disciplinary action against the member of staff, following the Staff Code Of Conduct and Disciplinary Policy.
- The Principal will decide whether it is appropriate to notify the police or anti-social behaviour coordinator in their LA of the action taken against a member of staff.

8.5. Use of illegal material:

- In the event that illegal material is found on the school's network, or evidence suggest that illegal material has been accessed, the police will be contacted.
- Incidents will be immediately reported to the Internet Watch Foundation and the police will be contacted if the illegal material is, or is suspected to be, a child sexual abuse image hosted anywhere in the world, a non-photographic child sexual abuse image hosted in the UK, or criminally obscene adult content hosted in the UK.
- If a child protection incident is suspected, the school's child protection procedure will be followed – the DSL and Principal will be informed and the police contacted.

9. Monitoring and review

9.1. The e-safety committee will evaluate and review this E-Safety Policy on an annual basis, taking into account the school's e-safety calendar, the latest developments in ICT and the feedback from staff/pupils.

9.2. This policy will also be reviewed on an annual basis by the governing body; any changes made to this policy will be communicated to all members of staff.

9.3. Members of staff are required to familiarise themselves with this policy as part of their induction programmes.