Blofield Primary School

E-Safety Policy

Reviewed by: Frazer Heasman and Teresa Doggett

Approved by Governors: 7th February 2022

Review: Spring term 2024



Contents:

Statement of intent

1. Legal framework
2. Use of the internet
3. Roles and responsibilities
4. E-safety control measures
5. Cyber bullying
6. Reporting misuse

Statement of intent

At Blofield Primary 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 recognise 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.

This policy will operate in conjunction with other important policies in our school, including our Anti-bullying Policy, Data Protection Policy (including GDPR), Child Protection and Safeguarding Policy, and Allegations Against Staff Policy.

1. Legal framework

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

- The Human Rights Act 1998
- The Data Protection Act 1998
- The Safeguarding Vulnerable Groups Act 2006
- The Education and Inspection Act 2006
- The Computer Misuse Act 1990, amended by the Police and Justice Act 2006
- The Prevent Duty (revised September 2016)
- General Data-Protection Regulation (GDPR) 2018

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 entitled to all pupils, though there are a number of controls required for the school to implement, which 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. These risks include:

- 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
- 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 computing coordinator is responsible for ensuring the day-to-day e-safety in our school, and managing any issues.

3.3. The headteacher is responsible for ensuring that the computing coordinator and any other relevant staff receive continuous professional development to allow them to fulfil their role and train other members of staff.

3.4. The computing coordinator will provide all relevant training and advice for members of staff on e-safety.

3.5. The headteacher will ensure there is a system in place which monitors and supports the computing coordinator, whose role is to carry out the monitoring of e-safety in the school.

3.6. The computing coordinator will regularly monitor the provision of e-safety in the school.

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

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

3.9. The computing coordinator 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.

3.10. The governing body computing link Governor will hold regular meetings with the computing subject leader to discuss the effectiveness of the e-safety provision, current issues, and to review incident logs.

3.11. The governing body will evaluate and review this E-safety Policy on a biannual basis.

3.12. The headteacher will review and amend this policy with the computing coordinator, taking into account new legislation and government guidance, and previously reported incidents to improve procedures.

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

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

3.15. All pupils will ensure they understand and adhere to the Acceptable Use Policy, which they must sign and return to the computing coordinator.

3.16. Parents/carers are responsible for ensuring their child understands how to use computer technology and other digital devices, appropriately.

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

3.18. The computing coordinator will ensure all staff understand how to use Microsoft teams effectively and confidently.

3.19. All staff are responsible for using Microsoft Teams safely and appropriately.

4. E-safety control measures

4.1. Educating pupils:

- An e-safety programme will be established and taught across the curriculum on a regular basis, ensuring 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.
- 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 all classrooms.
- Pupils are instructed to report any suspicious use of the internet and digital devices.

4.2. Educating staff:

- All staff will undergo e-safety training on a biannual basis to ensure they are aware of current e-safety issues and any changes to the provision of e-safety.
- All staff will undergo regular audits by the computing coordinator in order to identify areas of training need.
- All staff will employ methods of good practice and act as role models for pupils when using the internet and other digital devices.
- Any new staff are required to undergo e-safety training as part of their induction programme, ensuring they fully understand the E-safety Policy.

4.3. Internet access:

- Internet access will be allowed in line with the school's Acceptable Use Policy.
- Effective filtering systems are in place to eradicate potential risks to pupils through access to unsuitable websites, including terrorist and extremist material (in line with the Prevent Duty 2016).
- All staff will be vigilant of children's views and opinions when using the Internet and report any unusual or unacceptable behaviour to the Safeguarding Designated Professional (in line with the Prevent Duty 2016).
- Access is appropriate for the age of the children and managed by ICT Shared Services.
- Any requests by staff for websites to be added or removed from the filtering list must be first authorised by the headteacher.
- 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.

4.4. Email:

- Staff will be given approved email accounts and are only able to use these accounts, e.g.
    - Accounts from the .norfolk.sch.uk domain (e.g. office@school.norfolk.gov.uk)

- Use of personal email 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.
- Staff to pupil email communication must only take place via a school email address or from within the learning platform and will be monitored.
- Chain letters, spam and all other emails from unknown sources will be deleted without opening.

4.5. Social networking:

- 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 headteacher.
- 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.
- Staff are not permitted to communicate with pupils over social networking sites.

4.6. Published content on the school website and images:

- The headteacher will be responsible for the overall content of the website, and will ensure the content is appropriate and accurate.
- All contact details on the school website will be the phone, 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 images, though they must do so in accordance school policies in terms of the sharing and distribution of such. Staff will not take images using their personal equipment.

4.7. Mobile devices:

- The headteacher may authorise the use of mobile devices by a pupil where it is seen to be for safety or precautionary use.
- Mobile devices are not permitted to be used in the classroom by pupils or members of staff.
- The sending of inappropriate messages or images from mobile devices is prohibited.
- Mobile devices must not be used to take images 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.

4.8. Purple Mash:

- All children will have individual log in information and will only have access to their own individual account.
- All members of staff will have accounts and access to their own year groups, including children's individual accounts.
- The computing coordinator will have admin access and the ability to add, manage and delete users.
- Emails that are sent through the programme will be have to be approved by the class teacher or computing coordinator first.

5. Cyber bullying

5.1. 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.

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

5.3. 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.

5.4. 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.

5.5. 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.

5.6. The headteacher 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.

6. Reporting misuse

6.1. Misuse by pupils:

- Teachers have the power to discipline pupils who engage in misbehaviour with regard to internet use.
- Any instances of misuse should be immediately reported to a member of staff, who will then report this to the headteacher.
- Any pupil who does not adhere to the rules outlined in our Acceptable Use Policy and is found to be wilfully misusing the internet, will have a letter sent to their parents/carers 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 headteacher and will be issued once the pupil is on the school premises.
- Complaints of a child protection nature shall be dealt with in accordance with our Child Protection Policy.

6.2. Misuse by staff:

- Any misuse of the internet by a member of staff should be immediately reported to the headteacher.
- The headteacher will deal with such incidents in accordance with the Allegations Against Staff Policy, and may decide to take disciplinary action against the member of staff.
- The headteacher 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.