Bilsthorpe Flying High Academy

E-Safety Policy 2022-2023

Reviewed: October 2023

Next review due on: October 2024

Contents

1. Roles and Responsibilities

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

Governors:

- Governors are responsible for the approval of the Online Safety Policy.
- A member of the Governing Body has taken on the role of Safeguarding Governor and ensuring e-safety is prominent in school falls within this role.

Head teacher:

- The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day-to-day responsibility for online safety will be delegated to the Computing coordinator.
- The Headteacher and (at least) another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.
- The Headteacher is responsible for ensuring that the computing coordinator and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The Headteacher will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.

Computing coordinator:

- Takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies/documents
- Ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- Provides/organises training and advice for staff
- liaises with school governors
- Receives reports of online safety incidents and creates a log of incidents to inform future online safety developments
- Meets with Online Safety Governor to discuss current issues, review incident logs and filtering/change control logs
- Reports regularly to Senior Leadership Team

Teaching and support staff:

- They have an up-to-date awareness of online safety and of the current Online Safety Policy and practices.
- They have read, understood, and signed the Staff Acceptable Use Policy / Agreement in the Code of Conduct.
- They report any suspected misuse or problem to the Head teacher or a member of SLT.
- Online safety issues are embedded in all aspects of the curriculum.

- In lessons where internet 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.

2. Teaching and Learning

2.1 Why internet and digital communications are important

- The purpose of any technology in school is to raise educational standards, to promote achievement, to support the professional work of staff and to enhance the school's management functions.
- The school has a duty to provide students with quality internet access as part of their learning experience.
- Internet use is part of the statutory curriculum and a necessary tool for staff.
- Pupils will be educated in the safe, effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.
- They will be encouraged to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Pupils will be shown how to publish and present information appropriately to a wider audience.
- They will be taught what internet use is acceptable and what is not and be given clear objectives for use. These are also important transferable skills for their life out of school, including using mobile phones and other mobile devices.
- They will be taught how to report unpleasant internet content including Cyberbullying or unwanted contact.
- Issues such as Cyberbullying and e-safety will be built into the curriculum to encourage self –efficacy and resilience. Some children who have had problems or with additional needs may need additional support.

2.2 Managing Internet Access Information security system

- The school ICT system security will be reviewed regularly by the Flying High Trust.
- Virus protection will be updated regularly. Security strategies may be discussed with the Local Authority.

2.3 E-mail

- Pupils and staff may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a member of staff if they receive any offensive e-mail(s).
- Staff to pupil e-mail communication must only take place via a school e-mail address or from within a learning platform and will be monitored.
- All incoming e-mail should be treated as suspicious, and attachments not opened unless the author is known.
- The forwarding of chain letters is not permitted.

2.4 Published content and the school website

- The contact details on the school's website should be the school address. No staff or pupil's personal details will be published

- The headteacher/computing coordinator will have overall editorial responsibility to ensure that content is accurate and appropriate.

2.5 Publishing pupils' images and work

- Pupil's full names will be avoided on the website and learning platforms including blogs, forums especially if associated with a photograph.
- Parents should be clearly informed of the school policy on image taking and publishing.
- Photographs that include identifiable images of children should only be added to the school's website, X (formally known as Twitter), Facebook, Class Dojo accounts with consent from the parent/carer.

2.6 Social networking and personal publishing on the school learning platform

- The school will control access to social networking sites and consider how to educate pupils in their safe use. This may not mean blocking every site it may need monitoring and educating students in their use
- The school will encourage parents to support their children when setting up a social networking profile and offer help and guidance. This includes encouraging families to follow the terms and conditions specifying the appropriate age for using sites. Pupils will be advised never to give out personal details which may identify them or their location.

2.7 Managing filtering

- The school will work with the Local Authority and the Academy to ensure systems to protect pupils are reviewed and improved.
- Any unsuitable on-line material should be reported to the E-safety coordinator.
- Regular checks will be made to ensure the filtering methods are appropriate, effective and reasonable.
- A log will be kept and used to identify patterns and behaviours and therefore inform policy and educational interventions (log kept for staff record incidents).

2.8 Managing video conferencing

- Video conferencing will be appropriately supervised for the pupils' age.
- Pupils will always ask permission from the supervising teacher before making or receiving a video conference call.
- Video conferencing will use the educational broadband network to ensure quality of service and security.

2.9 Managing emerging technologies

- The school will examine emerging technologies for their educational benefit and carry out a risk assessment before use in school.
- Mobile phones and associated cameras will not be used in lessons or formal school time. They will be kept securely in the school office until home time.
- Care will be taken with the use of hand-held technologies in school which may not have the level of filtering required.

2.10 Project Evolve

- At Bilsthorpe Flying High Academy all our computing lessons begin with a discussion and activity on how to stay safe online. We use 'Project Evolve' to facilitate the teaching of E-

Safety through school, from F1 to Y6. This is evidenced in Computing floorbooks in each class.

- Class teachers deliver a 10-minute "mini-lesson" at the beginning of each Computing lesson to ensure children's knowledge of keeping safe online is current.

2.11 Digital Leaders

- At Bilsthorpe Flying High Academy, there are a group of Digital Leaders who roles are to promote the importance of e-safety and the Computing curriculum across school. This is a new project introduced in school this year by the e-safety lead and the children aim to attend training to develop and improve their skills.
- Being a Digital Leader is a popular role, and so there is always great interest amongst the rest of the school. They have a very high profile, with important duties in assemblies and computing lessons – promoting the importance of e-safety throughout this process.
- The aims of having Digital Leaders in school is to: support classmates in computing lessons and assemblies, be technology role models for our classmates, represent our school in the IT community, to help make our school the leading school in computing and to promote the importance of e-safety. We aim to help our classmates understand what this means and how they can keep safe.

3. Safety

3.1 Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

3.2 Authorising internet access

- All staff must read and sign the 'staff code of conduct' before using any school ICT resource
- The school will maintain a current record of all staff and pupils who are given access to school IT systems
- Parents will be asked to sign and return a consent form
- Access to the internet will be by adult demonstration with directly supervised access to specific online materials.

3.3 Assessing risks

- The school will take all reasonable precautions to prevent access to inappropriate material; however, it is not possible to guarantee that unsuitable material will never appear on a school computer.
- The school will monitor ICT use to establish if the e-safety policy is appropriate and effective.

3.4 Handling e-safety complaints

- Complaints of internet misuse will be dealt with by a senior member of staff.
- Complaints of misuse by staff will be referred to the Headteacher
- Any complaints of a child protection nature must be dealt with in accordance to child protection procedures (designated safeguarding lead will be informed immediately)
- Pupils and parents will be informed of the consequences and sanctions for pupils misusing the internet and this will be in line with the school's behaviour policy.

Inside School:

- Any incidents must be reported to a child's class teacher as soon as possible.
- If available, any evidence must be kept.
- Statements must be taken from all parties involved.
- A member of the Leadership Team must be informed and decide on the best course of action – this may include school-based sanctions, meetings with parents and, in the most severe incidents, the police may be involved.
- All incidents must be reported and logged.

Outside School:

- As soon as a member of staff is made aware of any e-safety incident, they must follow the guidance above.
- Parents should always be informed when e-safety incidents occur outside of school.

Children are regularly reminded of how to keep safe online and if any incidents were to occur, what they must do. They are also made aware of CEOP www.ceop.police.uk and Childline www.childline.org.uk 0800 1111.

3.5 Community use of the internet

- All use of the school internet connection by community and other organisations shall be in accordance with the e-safety policy.

3.6 The four C's:

- Pupils will be taught in all lessons to be critically aware of the materials and content that they access online and guided to validate the accuracy of the information that they are accessing. Staff will be vigilant in monitoring the content of the websites that the children are visiting when they are freely searching the internet. E.g. when researching. Illegal content is filtered by the broadband and filtering providers. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes. This filtering will ensure that children are safe from terrorist and extremist material when accessing the internet.
- Pupils will be protected from harmful interaction and contact with other uses through explicit teaching of how to use the internet safely as well as school filtering systems that control and limit the children's access when they are online.
- Pupils will be taught the appropriate way to conduct themselves online both through explicit teaching and modelling. Posters and displays will also reinforce the appropriate way to conduct oneself online in an age appropriate manner.
- Pupils will be made aware and protected from commerce risks through direct teaching within lessons. Commerce will also be blocked through the schools filtering systems.

4. Communicating the policy

4.1 Pupils

- Appropriate elements of the e-safety policy will be shared with pupils
- E-safety rules will be posted in all classrooms (display)
- Pupils will be informed that network and internet use will be monitored.
- Age appropriate curriculum opportunities will be used to ensure all pupils gain an awareness of e-safety. These will be addressed on a regular basis and modified as newer risks are identified.

4.2 Staff

- All staff will be given a copy of the E-safety policy and required to sign to acknowledge that they have read and understood the policy and agree to work within the guidelines.
- Staff should be aware that the system is monitored and that professional standards are expected.
- Staff monitoring the system will be supervised by senior management and have a clear procedure for reporting
- Staff will engage in training and CPD opportunities to ensure that they are up to date with E-Safety and online risks.

4.3 Parents

- Parents will be notified of the policy in newsletters, the school brochure and website
- All parents will be asked to sign the parent/pupil agreement when they register their children.
- Parents will be offered e-safety training to encourage them to support and encourage positive online activities with their children and help them to use the internet safely.

5. Acceptable Use Agreement

E-Safety: Staff Acceptable Use Agreement

Background and purpose

With access to rich dynamic content, connectivity across the globe, a platform for creativity and a place to engage in debate, digital technologies provide a powerful tool for learning. Digital technologies give staff opportunities to enhance children's learning in their care and enable staff to become more efficient in their work. The very nature of digital technologies means that they should be used with care and particular attention given to demonstrating appropriate behaviours and avoidance of misuse at all times. Professional integrity and strong moral purpose must be upheld at all times by staff. It is the duty of all staff members to ensure that children in their care get the very best start to the world of digital technology. This should include provision of a rich, robust online safety education for the children with clear reporting procedures for infringements to safeguarding. Having a transparent approach to using digital technology is a must. Additionally, staff should develop critical thinking in their children, along with strategies for avoiding unnecessary harm and strategies for dealing with online safety infringements. The school's internet, network and ICT systems and subscriptions to services should be used with the utmost professionalism at all times. The school will aim to provide its staff with secure systems which will have filtering, monitoring and virus protection included. Anyone with access to the systems should be aware that their use of the systems is monitored, and this can be used to form evidence should any suspected infringements occur.

Acceptable Use Agreement

By signing this agreement, you will have access to the school's systems and acknowledge that you agree to all the statements below. Additionally, that you have read and understand school policies which have a bearing on this agreement.

- I will demonstrate the value of the use of digital technologies in improving the outcomes for children in my care.
- I will educate children in my care in the safe use of digital technologies, acting on any online safety issues in accordance with the school's policies.
- I understand my use of the school's ICT systems/networks and internet are monitored.
- I recognise that whether within school or out of school, I must abide by the rules/statements set out in this document when using systems, accessing/transferring data that relate to the school or impact on my role within the school and wider community.
- I know what GDPR is and how this has a bearing on how I access, share, store and create data.
- Any data that I have access to away from school premises must be kept secure and used with specific purpose. As outlined in the school's data protection policy, it is my responsibility to ensure when accessing data remotely that I take every bit of reasonable care to ensure the integrity and security of the data is maintained.
- I understand that I am fully responsible for my behaviours both in and out of school and as such recognise that my digital communications, subscriptions and content I access can have a bearing on my professional role.
- I recognise that my social media activity can have a damaging impact on the school and children in my care at school if I fail to uphold my professional integrity at all times whilst using it.
- If I am contributing to the school's social media account(s) or website(s) I will follow all guidelines given to me, with particular care given to what images/video imagery and details can be uploaded.
- I will never upload images/video imagery of staff/pupils or other stakeholders to my personal social media accounts.
- I will inform the school at the earliest opportunity of any infringement both on and off site by myself. Furthermore, if I am concerned about others' behaviours/conduct, I will notify the school at the earliest opportunity.
- I will never deliberately access, upload or download illegal, inflammatory, obscene or inappropriate content that may cause harm or upset to others.
- I will never download or install software unless permission has been given by the appropriate contact at school.
- I shall keep all usernames and passwords safe and never share them.
- I will never leave equipment unattended which could leave data and information vulnerable; this extends to accessing data/services/content remotely.
- I understand that mobile devices, including smart watches, shall not be used, nor in my possession, during times of contact with children.
- Any school trips/outings or activities that require a mobile phone/camera will be provided by the school and any data collected on them will be used in accordance with school policies.
- At no point- will I use my own devices for capturing images/video or making contact with parents/carers.

Staff Name: _____

Staff Signature: _____

Date: _____

6. Code of Conduct

Staff / Governor Information systems code of conduct

To ensure that staff members are fully aware of their professional responsibilities when using information systems, they are asked to sign this code of conduct. Staff should consult the school's 'E-Safety Policy' for further information and clarification.

- ICT equipment and software are the property of the school and I understand that it is a criminal offence to use it for a purpose that is not permitted by the owner.
- I will ensure that the use of personal phones will be kept safe and secure and not used when in contact with the children.
- I will ensure that my use of technologies will always be compatible with my professional role.
- I understand that school ICT equipment must be used responsibly and may not be used for private purposes, without specific permission from the Head Teacher.
- I understand that the school may monitor my information systems and internet use to ensure policy compliance.
- I will respect system security and I will not disclose any password or security information to anyone other than an authorised person.
- I will not install any software or hardware without permission.
- I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will respect copyright and intellectual property rights.
- I will report any incidents of concern to the designated school e-safety leader or child protection officer.
- I will ensure that any electronic communications with pupils are appropriate to my professional role.
- I will promote e-safety with pupils in my care and will help them to develop a responsible attitude to system use and the content they access or create.
- If I use social networking websites, I understand that I must not mention the school in a negative or derogatory way and that failure to comply with this can result in disciplinary action.

The school may exercise its right to monitor the use of the school's technology, including internet access and e-mail. The school will take the necessary action where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

I have read, understood and agree with the information systems code of conduct

Signed: _____ Name: _____ Date: _____

7. Pupil Incidents

Pupil Incidents	Refer to class teacher	Refer to phase leader	Refer to the head teacher	Refer to the police	Refer to the technical support staff from the LEA for action refiltering/	Inform parents/carers	Removal of network/ internet access rights	Warning	Further sanction e.g. detention/ exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities)		x	x	x	x		x		x
Unauthorised use of non-educational sites during lessons			x		x		x		x
Unauthorised / inappropriate use of mobile phone / digital camera / other mobile device			x		x	x	x		x
Unauthorised / inappropriate use of social media / messaging apps / personal email			x		x	x	x		x
Unauthorised downloading or uploading of files			x		x	x	x		x
Allowing others to access school network by sharing username and passwords			x		x	x	x		x
Attempting to access or accessing the school network, using the account of a member of staff			x		x	x			x
Corrupting or destroying the data of other users			x		x	x			x
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature			x		x	x			x
Continued infringements of the above, following previous warnings or sanctions			x		x	x			x
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school			x		x	x	x		x
Using proxy sites or other means to subvert the school's filtering system			x		x	x			x
Accidentally accessing offensive or pornographic material and failing to report the incident			x	x	x	x	x		x
Deliberately accessing or trying to access offensive or pornographic material			x	x	x	x	x		x
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act			x	x	x	x	x		x

8. Links to other policies

- Safeguarding and Child protection Policy
- Computing Policy
- Social Media and Guidance Policy
- GDPR Policy
- Behaviour Policy
- Staff Code of Conduct

Keeping Children Safe in Education September 2023

Online Safety within 'Keeping Children Safe in Education' 2023:

• Specific online safety content has been strengthened to ensure online safety is clearly viewed as part of a school and college's statutory safeguarding responsibilities.

• The DSL continues to have overall responsibility for online safety; they can be supported by appropriately trained deputies and should liaise with other staff as appropriate, but this responsibility cannot be delegated.

• DSLs should continue to evidence that they have accessed appropriate training and/or support to ensure they understand the unique risks associated with online safety, can recognise the additional risks learners with SEN and disabilities (SEND) face online, and have the relevant knowledge and up to date capability required to keep children safe online.

• All staff should continue to be provided with online safety information and training at induction, and the importance of receiving online safety training as part of regular (at least annual) child protection training and updates has been empathised. Children should be taught about online safety, including as part of statutory Relationships and Sex Education (RSE), but schools and colleges should recognise that a one size fits all approach may not be appropriate and a more personalised or contextualised approach for more vulnerable children e.g., victims of abuse and SEND, may be needed.

• Schools and colleges should ensure their child protection policy and wider safeguarding policies specifically address online safety, especially with regards to online peer on peer abuse, relationships on social media and the use of mobile and smart technology.

• KCSIE 2023 references four areas of risk online: content, contact, conduct and commerce.

• Online safety should be considered to be part of your statutory safeguarding responsibilities and requires a whole school/college approach.

• Ensure your staff behaviour policy specifically covers acceptable use of technologies, including the use of mobile devices, staff/pupil relationships and communications, including the use of social media.

• Work with curriculum leads (especially RSE leads) to ensure there is a range of opportunities within the curriculum for children to be taught about online safety in a way that is appropriate to their age and needs.

• Ensure all staff are provided with appropriate and up-to-date online safety information and training at induction, and as part of regular child protection training and updates.

• Ensure all staff are aware of the policies and procedures to follow with regards to responding to online safety concerns, including online peer on peer abuse issues.

• Ensure the DSL is recognised as having overall responsibility for online safety and that they access appropriate training and support to enable them to keep up to date.

• DSLs from all school and college types should ensure they have accessed the UKCIS 'Sharing nudes and semi-nudes: advice for education settings working with children and young people' guidance and are familiar with its content and when it should be followed.

• Ensure appropriate filtering and monitoring approaches are in place which are suitable for the local context and use of technology.

• Remote learning should be implemented in a safe and secure way.

• There should be regular and appropriate parental engagement in online safety, however specific concerns should be responded to in line with child protection policies.

• Online safety approaches should be regularly reviewed and updated as required.

This E-safety policy was revised by: Brogan Evans

On (date): 03.10.2023

It was approved by the Governors on: _____