

## Beacon Federation Policy Document

## E-Safety Policy

|  |  |
| --- | --- |
| Written / Updated | October 2019 |
| Approved by Governors | N/A |
| Review date | October 2022 |

***NB – 2019-20 is a transitionary year for the Federation. This policy will be adopted gradually by all three schools over the course of the year with full implementation from September 2020. Not all elements of this policy will be seen consistently across the Federation until that date.***

**Introduction**

At The Beacon Federation, we recognise that the internet is an essential resource to support teaching and learning and is a part of the statutory curriculum and a necessary tool for both staff and pupils. As such, we are committed to ensuring that children learn how to use Computers, ICT and modern technologies safely so that they:

* Are able to use ICT safely to support their learning both at school and home.
* Use ICT as a tool for communication and understand how to do so in a safe manner.
* Understand the dangers of online communication and know what to do if they feel unsafe when using ICT technology.
* Are prepared for the constant changes in the world of technology and understand how to use all new and emerging technologies safely.

This policy outlines the steps taken by The Beacon Federation to ensure safe internet use by its pupils in school, but the schools also proactively encourage children to develop a safe approach to ICT use and communication outside of its confines.

**The Law**

The e-safety policy has been written by The Beacon Federation using government guidance. However, as legislation is often amended and new regulations introduced, references made in this policy may be superseded. For an up to date list of legislation applying to schools please refer to the Department for Education website at: [www.education.gov.uk/schools](http://www.education.gov.uk/schools).

**Roles and Responsibilities**

E-safety is an important aspect of Safeguarding. As such, the Executive Headteacher and governors have the ultimate responsibility to ensure that that the policy and practices are embedded and monitored.

**The Governors and Executive Headteacher will:**

* Ensure that the E-Safety Policy is implemented, communicated and monitored.
* Ensure that a Computing Policy outlining ICT and e-safety as integral parts of the school curriculum, is implemented, communicated and monitored.
* Ensure that the school has a sufficient filtering software to protect children from potentially damaging material.

**The Designated Safeguarding Lead will:**

* Ensure that all staff are trained on the aspects of e-safety periodically as part of safeguarding training.
* Include e-safety as part of the Safeguarding Refresher training.
* Staff are regularly mailed the Safeguarding updates from the NSPCC and the Babcock Safeguarding Team.
* Work with the CAP Team from Devon and NSCC workshops for staff and pupils.
* Investigate any reports of cyber-bullying or inappropriate communication.

**Teachers and Staff will:**

* Read and maintain awareness of the Computing and E-Safety Policies.
* Participate in all e-safety training offered.
* Adhere to the Acceptable Use Agreement.
* Promote and teach e-safety as part of the computing curriculum.
* Monitor and supervise pupils’ internet usage and use of other IT resources
* Only download attachments/material onto the school system if they are from a trusted source.
* When capturing images, videos or sound clips of children, only use school cameras or recording devices.
* Never use personal mobile phones or other devices to record images.

**The Technician will:**

* Regularly review and update the schools’ system security and virus protection, liaising with the LEA in doing so.
* Ensure that regular checks are made to ensure that filtering methods selected are appropriate, effective and reasonable.
* Deal appropriately with any reports of unsuitable or illegal sites or material being discovered.

**Teaching and Learning**

Internet use will enhance learning as follows:

* Pupils will be taught the importance of safe internet use and give clear guidelines and objectives about what is acceptable.
* Pupils will be educated in the effective use of the internet for research, including the skills of knowledge location, retrieval and evaluation.
* Pupils will be shown how to publish and present information to a wider audience in a safe manner.
* Pupils will be taught the importance of cross checking information before accepting its accuracy, and of following copywright laws.
* All forms of bullying, including cyberbullying will be taken seriously, reported to the Executive Headteacher and logged in the appropriate file located in the office.

**Managing Internet Access**

**Information system security**

* The schools internet access is provided through the South West Grid for Learning (SWGfL) which is designed for pupil use and includes filtering appropriate to the school.
* Computer system security and virus protection will be reviewed regularly by the Technician.
* If staff or pupils discover unsuitable sites, the URL and content will be reported to the computing team who will contact the Technician.

**E-mail**

* Pupils may only use an approved e-mail account on the school system.
* Pupils must immediately tell a teacher if they receive offensive e-mail.
* Pupils must not reveal their personal details or those of others, or arrange to meet anyone they have been in contact with.
* Emails sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter on school headed paper.
* 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.

**Published content and school website**

* Staff or pupil personal contact information will not be published.

(The contact details given will be [admin@manor.devon.sch.uk](mailto:admin@manor.devon.sch.uk), [admin@ugborough-primary.devon.sch.uk](mailto:admin@ugborough-primary.devon.sch.uk) or [office@ermington.devon.sch.uk](mailto:office@ermington.devon.sch.uk) respective for each school)

* Written permission from parents or carers will be obtained before photographs of pupils are published on the school website. Photographs that include pupils will be selected carefully so that their image cannot be misused.
* Pupils’ full names will not be used anywhere on a school website or other on-line space, particularly in association with photographs. Website photographs will be selected carefully to ensure individual pupils cannot be identified by name.

**Social networking and personal publishing**

* The school will control access to social networking sites, and will educate pupils in their safe use.
* Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location.
* Pupils and parents will be advised that the use of social networking spaces outside school brings a range of dangers for primary aged pupils.
* Pupils will be advised to use nicknames and avatars when using social networks.
* Schools will ensure that staff and pupils are aware that the use of internet derived materials should comply with current copyright laws.
* Specific lessons will be included to teach all pupils how to read for information from web resources.
* Staff should exercise caution, sound judgement, and common sense when using social media sites.
* Employees of the school should not communicate with students on roll or former students (until they are over 18) through social media sites, and should exercise extreme caution when befriending or communicating with parents of children enrolled at school.
* No reference should be made via social media to students / pupils, parents/carers/school staff or issues / situations or people related to the school.
* Personal opinions should not be attributed to the school.
* Security settings on personal social media profiles should be regularly

checked to minimise risk of loss of personal information.

**Managing Filters**

* The Technician will work with SWGfL to ensure systems to protect pupils are reviewed and improved.
* If staff or pupils come across unsuitable material or illegal sites, the URL (address) and content must be reported to the Technician and the Executive Headteacher immediately.
* The Computing team will ensure that the Technicianmakes regular checks to ensure that filtering methods selected are appropriate, effective and reasonable.

**Managing videoconferencing and webcam use**

* Videoconferencing should use the SWGfL broadband network to ensure quality of service and security.
* Pupils must be accompanied by a member of staff before throughout any videoconferencing call.

**Managing emerging technologies**

* Emerging technologies will be examined for educational benefits by the Computing Team, and a risk assessment will be carried out before use is allowed.
* Technologies such as mobile phones with wireless internet access can bypass school filtering systems and present a new route to undesirable material and communication. Pupils are not allowed, therefore, to have mobile phones in school and must hand these in to the office at the start of the school day.
* The sending of abusive or inappropriate text messages or files is forbidden.
* Appropriate use of mobile phones will be taught to pupils as part of their e-safety programme.
* Staff must not use their own mobile phones in the presence of pupils and they should be turned off during lesson time. Staff are only permitted to use mobile phones in the school offices or staff room.

**Protecting personal data**

* Personal data will be recorded, processed, transferred and made available according to the General Data Protection Regulations 2016.

**Policy Decisions**

**Authorising Internet access**

* All staff will be provided with the E-Safety Policy, and its importance explained.
* All staff must read and sign the “Code of Conduct for Computing” before using the resources.
* All staff will be given the SWGfL Internet Acceptable Usage Policy.
* The school will maintain a current record of all staff and pupils who are granted access to the school computing systems.
* All pupil internet access will be supervised by an adult.
* Parents will be asked to sign and return a consent form.
* Any person not directly employed by the school will be asked to sign the “Code of Conduct for Computing” before being allowed to access the internet from the school site.
* Staff development in safe and responsible internet use and on the school Internet policy will be provided as required.

**Assessing risks**

The Federation will take reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the school network. Neither the Federation nor Devon LEA can accept liability for any material accessed, or any consequences of internet access.

**Handling e-safety complaints**

* Complaints of internet misuse will be dealt with by the Designated Safeguarding Officer.
* Any complaint about staff misuse must be referred to the Executive Headteacher.
* Complaints of a child protection nature must be dealt with in accordance with the school’s child protection procedures.
* The complaints procedure is available on school websites.
* Parents and pupils will need to work in partnership with staff to resolve issues.
* There may be occasions when the police must be contacted. Early contact could be made to establish the legal position and discuss strategies.

**Introducing the E-Safety policy to pupils**

* All children begin the academic year learning about e-safety and follow the SMART rules (Safe, Meeting, Accepting, Reliable) to keep them safe when using the internet.
* E-Safety rules will be displayed in the classrooms and discussed with pupils regularly to remind the children how to use the internet safely and responsibly. Reminders about responsible and safe use should precede internet access.
* Pupils will be informed that network and internet use will be monitored and appropriately followed up.
* E-safety training will be embedded within the computing and PSHE curriculums, covering both school and home use. This will include the necessity of keeping personal information safe, how to use mobile technologies appropriately and using online communication appropriately.
* An online gaming guidance is shared with all children and parents outling the need and how to stay safe when playing online games.

**Staff and the e-safety policy**

* All staff will be given the e-safety policy and its importance explained.
* Staff must be informed that network and internet traffic can be monitored and traced to the individual user.
* Staff will use a child friendly search engine when accessing the web with Foundation and KS1 children, however children in KS2 will be taught how to safely search the internet using engines such as Google.
* Children must be monitored by staff at all times, and never left alone when using the internet.

**Enlisting parents’ and carers’ support**

* This policy will be available on the school websites. Guidance is available on the school website that directs parents to best practise and supporting articles.
* Information will be provided to parents periodically about how to work with the school to ensure e-safety both within school and home.
* A partnership approach with parents will be encouraged.
* The school provide parents with e-safety resources on request.
* New parents will be asked to sign the internet permission form.

**Pupil Acceptable Use Agreement/e-Safety Rules**

Dear Parent/Carer

Computing has become an important part of learning in our school. We expect all children to be safe and responsible when using any equipment or resources. Please discuss these e-safety rules with your child. If you have any concerns, please see the E-Safety Policy on our website, or contact the school.

* I will only use computing in school for school purposes.
* I will only use my class email address.
* I will make sure that all contacts with other children and adults are responsible.
* I will not deliberately look for, save or send anything that could be unpleasant or hurtful. If I accidentally find anything like this I will turn off my monitor and tell my teacher immediately.
* I will not send anything to children or adults that could be considered unpleasant or hurtful.
* I will not give out my own details such as my name, phone number or address.
* I will not arrange to meet someone unless this is part of a school project approved by my teacher, and a responsible adult comes with me.
* I will be responsible for my behaviour when using computing because I know that these rules are to keep me safe.
* I know that my use of computing can be checked and that my parent/ carer contacted if a member of school staff is concerned about my e-safety.

**E-Safety Agreement**

Name of child ………………………………………………………………

Class……………………………………………………

We have discussed this and my child agrees to follow the e-Safety rules and to support the safe use of computing at The Beacon Federation.

Parent/ Carer Signature ………………………………………………….……

Date ……………………………….

Dear Parents /Carers

**Responsible Internet Use**

As part of your child’s curriculum and the development of their Computing skills, The Beacon Federation provides supervised access to the internet. We believe it is an essential skill for children as they grow up in the world.

All children begin the academic year learning about e-safety and follow the SMART rules to keep them safe when using the internet. These are displayed in the computer suite to remind the children how to use the internet safely and responsibly.

Our school internet provider is the SWGfL, which operates a filtering system that restricts access to inappropriate materials. However, whilst every endeavour is made to ensure that suitable restrictions are placed on the ability of children to access inappropriate materials, the school cannot be held responsible for the nature or content of materials accessed through the internet. The school will not be liable for any damages arising from your child’s use of the internet facilities.

Please would you read the attached Acceptable Use agreement and sign and return the consent form so that your child may use the Internet at school.

Should you wish to discuss any aspect of internet use please contact the school.

Yours sincerely

**Code of Conduct for Computing at The Beacon Federation**

**To ensure that members of staff are fully aware of their professional responsibilities when using information systems and when communicating with pupils, they are asked to sign this code of conduct. Members of staff should consult the school’s e-safety policy for further information and clarification.**

* I understand that it is a criminal offence to use a school computing system for a purpose not permitted by its owner.
* I understand that school information systems may not be used for private purposes without specific permission from the Executive Headteacher.
* I understand that my use of school information systems, internet and email may be monitored and recorded 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 system manager.
* I will not install any software or hardware without permission.
* I will ensure that personal data is stored securely 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 regarding children’s safety to the Designated Child Protection Coordinator or Executive Headteacher.
* I will ensure that electronic communications with pupils including email, IM and social networking are compatible with my professional role and that messages cannot be misunderstood or misinterpreted.
* I will promote e-safety with students in my care and will help them to develop a responsible attitude to system use, communications and publishing.

The school may exercise its right to monitor the use of the school’s information systems and internet access, to intercept e-mail and to delete inappropriate materials 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 accept the Staff Code of Conduct for Computing.**

Signed: …………..…………..… Capitals: …………....………………Date: ……………

Accepted for school: ……………………… Capitals: …………………………. ……………