



Forest Edge Learning Federation

E-Safety Policy

Name of School:	Breamore CE Primary, Hale Primary and Hyde CE Primary
Name of Responsible Manager/Headteacher:	Tracy Allen – Executive Headteacher
Date Policy approved and adopted:	January 2024
Date Due for review:	January 2025

*Our children will be **globally-aware, confident, successful learners** who, within our ambitious and forward thinking environments, will develop a secure sense of **self-worth***

This policy should be read alongside The Forest Edge Learning Federation's policies and procedures on child protection and safeguarding.

The purpose of this policy statement

The purpose of this policy statement is to:

- ensure the safety and wellbeing of children and young people is paramount when adults, young people or children are using the internet, social media or mobile devices
- provide staff and volunteers with the overarching principles that guide our approach to online safety
- ensure that, as an organisation, we operate in line with our values and within the law in terms of how we use online devices.

This policy applies to all members of the Forest Edge Learning Federation community (including staff, learners, volunteers, parents and carers, visitors, community users) who have access to and are users of school digital systems, both in and out of the school. It also applies to the use of personal digital technology on the school site (where allowed).

Legal framework

This policy has been drawn up on the basis of legislation, policy and guidance that seeks to protect children in England. Summaries of the key legislation and guidance are available on:

- [Online abuse](#)
- [Bullying](#)
- [Child protection.](#)

We believe that:

- children and young people should never experience abuse of any kind
- children should be able to use the internet for education and personal development, but safeguards need to be in place to ensure they are kept safe at all times.

We recognise that:

- the online world provides everyone with many opportunities; however it can also present risks and challenges
- we have a duty to ensure that all children, young people and adults involved in our organisation are protected from potential harm online
- we have a responsibility to help keep children and young people safe online, whether or not they are using Forest Edge Learning Federation's network and devices
- working in partnership with children, young people, their parents, carers and other agencies is essential in promoting young people's welfare and in helping young people to be responsible in their approach to online safety


- all children, regardless of age, disability, gender reassignment, race, religion or belief, sex or sexual orientation, have the right to equal protection from all types of harm or abuse.

We will seek to keep children and young people safe by:

- appointing a computing lead who, as part of their role, is an online safety coordinator
- providing clear and specific directions to staff and volunteers on how to behave online through our [FELF Acceptable Use of ICT Policy](#)
- supporting and encouraging the young people using our service to use the internet, social media and mobile phones in a way that keeps them safe and shows respect for others
- supporting and encouraging parents and carers to do what they can to keep their children safe online
- developing an online safety agreement (Appendix 1 & 2) for use with young people and their parents or carers
- developing clear and robust procedures to enable us to respond appropriately to any incidents of inappropriate online behaviour, whether by an adult or a child or young person
- reviewing and updating the security of our information systems regularly
- ensuring that usernames, logins, email accounts and passwords are used effectively
- ensuring personal information about the adults and children who are involved in our organisation is held securely and shared only as appropriate
- ensuring that images of children, young people and families are used only after their written permission has been obtained, and only for the purpose for which consent has been given
- providing supervision, support and training for staff and volunteers about online safety
- examining and risk assessing any social media platforms and new technologies before they are used within the organisation.

Handling e-safety complaints:

The federation will take all reasonable precautions to ensure online safety for all users but recognises that incidents may occur inside and outside of the schools (with impact on the schools) which will need intervention.

The federation will make the  360 safe - Online safety incident flowchart available to staff to support the decision-making process for dealing with online safety incidents.

- Complaints of internal internet misuse will be dealt with by the Executive Headteacher.
- 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 school child protection procedures.
- Pupils and parents will be informed of the complaints procedure.

- Discussions will be held with the community police to establish procedures for handling potentially illegal issues.

If online abuse occurs, we will respond to it by:

- having clear and robust safeguarding procedures in place for responding to abuse (including online abuse)
- providing support and training for all staff and volunteers on dealing with all forms of abuse, including bullying or cyberbullying, emotional abuse, sexting, sexual abuse and sexual exploitation
- making sure our response takes the needs of the person experiencing abuse, any bystanders and our organisation as a whole into account
- reviewing the plan developed to address online abuse at regular intervals, in order to ensure that any problems have been resolved in the long term.

Roles and responsibilities:

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

Governors:

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the governors on the Learning and Achievement Committee and the Safeguarding Governor receiving regular information about e-safety incidents and monitoring reports.

Headteacher and Senior Leaders:

- The Executive Headteacher and Executive Deputy Headteacher are responsible for ensuring the safety (including e-safety) of members of the federation, though the day-to-day responsibility for e-safety will be delegated to the Online safety coordinator/Computing Lead.
- The Executive Headteacher/Senior Leadership team are responsible for ensuring that the Online safety coordinator and other relevant staff receive suitable CPD training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.
- The Executive Headteacher/Senior Leadership Team will ensure that there is a system in place to allow for monitoring and support of those in the federation 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 Senior Leadership Team will receive monitoring reports from the Online Safety coordinator.
- The Executive Headteacher and Senior Leadership team should be aware of the procedures to be followed in the event of a serious e- safety allegation being made against a member of staff.

Online Safety Coordinators / Computing Lead

- Takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the federation e-safety policies / documents.

- Ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- Provide training and advice for staff
- Liaise with the federation's ICT technical staff
- Receive reports of e-safety incidents and create a log of incidents to inform future e-safety developments.
- Meets with the safeguarding governor to discuss current issues and review incident logs
- Attends relevant meetings.
- Ensure all classes have a key stage relevant E-safety poster (Appendix 3) and an e-safety charter (Appendix 1) signed by the children on display.

Federation Network Provider:

- That the federation's ICT infrastructure is secure and is not open to misuse or malicious attack as well as off- site access
- That the federation meets the e-safety technical requirements
- That users may only access the federation's networks through a properly enforced password protection policy, in which passwords are regularly changed
- They keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant

School's Broadband Provider:

- Scheduled safeguarding and prevent reports sent to school senior leadership team.

Teaching and Support Staff

- They have an up to date awareness of e-safety matters and of the current e-safety policy and procedures
- They have read, understood and signed the school '[Staff Acceptable Use of ICT Policy](#)'
- They report any suspected misuse or problem to the Online safety coordinator or Headteacher for investigation
- Digital communications with pupils (VLE-Virtual Learning Environment) should be on a professional level and only carried out using official federation systems
- E-safety issues are embedded in all aspects of the curriculum and other federation activities- Use of Digital Citizenship lessons as well as involvement in Safer Internet Day should ensure this is happening.
- Pupils follow the federation e-safety and acceptable use policy
- Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- Ensure their class has a key stage relevant E-safety poster (Appendix 3) and an e-safety charter (Appendix 1) signed by the children on display.
- They monitor computing activity in lessons, extracurricular and extended federation activities
- They are aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current federation 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. Where learners are allowed to freely search the

internet, staff should be vigilant in supervising the learners and monitoring the content of the websites the young people visit.

- That processes are in place for dealing with any unsuitable material that is found in internet searches. This is highly unlikely due to the federation's filtering policy but any breach should be reported immediately to the Headteacher.

Designated Safeguarding Leads:

The Designated Safeguarding Leads (DSLs) should be trained in e-safety issues and be aware of the potential for serious child protection issues to arise from:

- Sharing of personal data
- Access to illegal / inappropriate materials
- Inappropriate on-line contact with adults / strangers
- Potential or actual incidents of grooming
- Cyber-bullying

Pupils:






- Are responsible for using the federation's ICT systems in accordance with the 'Pupil Acceptable Use Policy'(Appendix 1), which they will be expected to sign as a class charter and revisit every year, before being given access to federation systems.
- 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.
- Will be expected to know and understand federation policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand federation policies on the taking / use of images and on cyber-bullying.
- Should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the federation's E-Safety Policy covers their actions out of school, if related to their membership of the federation.


Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The federation will therefore take every available opportunity to help parents understand these issues through parents' evenings, letters and the website. Parents and carers will be responsible for:

- Endorsing (by signature) the Parent/Carer Agreement (Appendix 2) included in the new starter consent booklet when joining the Federation or I will confirm my acceptance by ticking the relevant consent on Arbor.
- Related policies and procedures

This policy statement should be read alongside our organisational policies and procedures, including:

-  FELF Child Protection Policy 2022.pdf
-  FELF Safeguarding policy 2022.pdf
-  Anti Bullying Policy FELF 2022.pdf
-  FELF Social Media Policy 21.pdf
-  FELF Social Media Code of Conduct for Parents .pdf

-  FELF code of conduct 21 .pdf
- procedures for responding to concerns about a child or young person's wellbeing
- dealing with allegations of abuse made against a child or young person
- managing allegations against staff and volunteers
- photography and image sharing guidance.

Contact details

Online Safety Co-ordinator

Name: Megan Coombes

Email: megan.coombes@forestedge.org.uk

Designated Safeguarding Lead

Name: Tracy Allen

Email: tracy.allen@forestedge.org.uk

NSPCC Helpline

0808 800 5000

We are committed to reviewing our policy and good practice annually.

Appendix

(Appendix 1) Pupil Agreement

This is how I stay safe when I use electric devices (Computers, Laptops, Chromebooks, I pads, Tablets, ect) :

- I will keep my passwords safe and not share them with my friends.
- I will only use the computer for things my teacher has told me to.
- I will make sure that all the messages I send are polite.
- I will tell a teacher if I see something that makes me feel scared or uncomfortable on the screen.
- I will not reply to any nasty message or anything that makes me feel uncomfortable.
- I will not tell people about myself online (I will not tell them my name, mobile phone number, anything about my home, family, pets and school).
- In school, I will only use my school email.
- I will only email people I know or who my teacher says it is okay to email.
- I will never agree to meet a stranger.
- I will not put photographs of myself online without asking a teacher.
- I know that my teacher can check what I do online and that if I break the rules I might not be allowed to use a computer.

Signed _____

(Appendix 2) Parent/Carer Agreement

School Policy

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies are powerful tools, which open up new opportunities for everyone.

These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- That young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.
- That school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

The school will try to ensure that pupils will have good access to digital technologies to enhance their learning and will, in return, expect the pupils to agree to be responsible users.

Parent / Carer Signature

As the parent / carer, I understand that the school has discussed the Acceptable Use Agreement with my child as part of the whole school commitment to e-Safety both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and computing systems.

I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the Internet.

I understand that my child's activity on the computing systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's e-Safety.

Name of Pupil _____

Class _____

Signed (parent/carer) _____

Date _____

(Appendix 3) E-Safety Classroom Poster

Key Stage 1 Poster



Internet Safety

S **SPEAK**
to somebody if you need help.

A **ASK**
an adult before going online.

F **FRIENDS**
are real people we know.

E **ENJOY**
Play, have fun and stay safe.

Speak to:

if you are worried about anything.



Copyright 2017 www.esafety-adviser.com e-safety adviser

Key Stage 2 Poster

S **M** **A** **R** **T**

SHARE RESPONSIBLY
We all love to share photographs, fun things we're doing and much more.
Be careful what you share and always ask permission if somebody else is in the photo or video.

MANAGE your PRIVACY
If you're using apps that can communicate with others, turn on privacy.
Only let people you really know follow you unless you've asked permission from your parents.

ASK for HELP
Don't ever be worried about asking for help from someone you trust.
You will NOT be judged.

RESPECT OTHERS
Be kind.
Other people may have different opinions from you.
That's okay, but if they become abusive, take screenshots, block and report and tell an adult.

THINK CRITICALLY
TRUST your INSTINCT
Is it true?
Does that person really know me?
Has that really happened?
Always question!

If anything worries you, or if you need help with something, speak to:

Copyright 2017 e-safety adviser www.esafety-adviser.com

