Best Futures School

Where Children Come First

E-SAFETY POLICY

Date updated – May 2025
Produced by – Rose Best
Lead – Dawn Best
CIC Input by – Rose Best and Steve Davies
Status – Current
Review Date – May 2026 or sooner if legislation is updated

Table of Contents

1: Context

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications 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.

Safeguarding is a serious matter; in our school we use technology and the Internet extensively across all areas of the curriculum. Online safeguarding, known as e-safety is an area that is constantly evolving and as such this policy will be reviewed on an annual basis or in response to an e-safety incident, whichever is sooner.

2: Aims / Objectives

Teaching, learning, personal development and well-being should be enhanced through:

- The monitoring of a safe ICT learning environment through which pupils can develop their skills and knowledge,
- Supporting everyone in being responsible users of ICT, aware of their rights and responsibilities,

- Equipping users with the skills and knowledge to stay safe while using the internet and other communications technologies for educational, personal and recreational use,
- Ensuring that parents and carers are aware of the importance of e-safety and are involved in the education and guidance of pupils with regard to their on-line behaviour.

3: Learning

A planned e-safety curriculum will ensure that:

- Pupils are taught what Internet use is acceptable and what is not and given clear objectives for internet use.
- Pupils are educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- Pupils are shown how to publish and present information, safely, to a wider audience.
- Pupils are taught to acknowledge the source of information used and to respect copyright, when using the internet.
- Pupils are taught the importance of e-safety methods of searching the internet and the importance of cross-checking information before accepting its accuracy.
- Pupils are taught how to report unpleasant, inappropriate and/or illegal internet content
- Pupils are taught about the safe use of social networking sites.
- Pupils are taught never to give out personal details of any kind which may identify them, their friends or their location.
- Pupils are taught the reasons why personal photos/videos should not be posted on any social network space without considering how the photo/video could be used now or in the future.
- Pupils are taught about security and encouraged to set passwords, to deny access to unknown individuals and to block unwanted communications. Pupils should only invite known friends and deny access to others.

4: Managing equipment, system security, monitoring and filtering

Antivirus system is used to protect Windows-based machines. Any potentially inappropriate material accessed through the school's network by pupils or staff, must be reported to the Executive Principal, Designated Safeguarding Lead and Data protection officer. Physical access to servers, switches and wireless systems are restricted.
The pupils have access to a children's Fire Kindle tablet, which does not have access to the internet. Pupils are able to use school PCs and are supervised at all times.

Virtual Reality Headset

We have a new Virtual Reality Headset (VR) which is used alongside SEMH sessions and immersive learning. This is restricted in the same way as other technology in the school and has the same limited access to the internet. Use of the VR set is always supervised, safety precautions in place. VR options are restricted to appropriate applications such as tours of historic landmarks/sites/tourism destinations, calming/meditation exercises, and physical activities. For example BeatSaber which is a dancing app which we use in wellbeing sessions as part of 5 steps to wellbeing.

Staff set up the specific task or activity, so the search bar isn't required or access by pupils.
Appropriate area in a safe space is set up by staff prior to starting, some activities can be stationary or seated. Staff complete dynamic risk assessment for each activity and each pupil, specific to their needs.

There is information available from the NSPCC regarding Headsets and how to encourage safe usage for families as headsets grow increasingly popular
Please see this link Virtual Reality Headsets | NSPCC

5: Email Filtering

We use the in-built Microsoft Office 365 software that aims to prevent any infected email to be sent from the school, or to be received by the school. Infected is defined as: an email that contains a virus or script (i.e. malware) that could be damaging or destructive to data; spam email such as a phishing message

6: Mobile Technology

As the proliferation of mobile technology continues to expand, we will continue to ensure these devices offer the same level of filtering protection as more traditional technology. All mobile devices brought to school by the pupils will be kept in the office until the end of the school day.

7: Publishing content

Staff or pupil personal contact information will not be published. The contact details given online is those of the school. The Executive Principal will take overall editorial responsibility and ensure that published content is accurate and appropriate. Photographs and videos that include pupils will be selected carefully so that images of individual pupils cannot be misused. Pupils' full names will not be used anywhere on the school Web site or other on-line presence, particularly in association with photographs and/or videos. Written permission, using the approved permission form, from parents or carers will be obtained before photographs/videos of pupils are published on the school website or other on-line presence. For more information, see our Media Policy in the Policies and Procedures Folder.

8: Managing emerging technologies

Emerging technologies will be examined for their educational benefit and potential risks, before use in the school is allowed.

9: Staff, Board of CIC and Visitors

All staff, Board of CIC and visitors will be given access to the e-safety policy. Users are informed that network and Internet traffic can be monitored and traced to the individual user. Senior staff will ensure access to training, information and support is available for all staff and CIC members as appropriate. All staff, CIC members and visitors have a responsibility to seek clarification or training, where they identify areas of e-safety as a training need.

10: Parents/carers and the wider family

Parents/carers will be informed that whilst the school will take all reasonable precautions to prevent access to inappropriate material, 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 device connected to the school network. Links to national events such as: Anti-bullying Week and Safer Internet Day are used to raise the profile of e-safety.

Best Futures school website shares information regarding e-safety through the Parents and Carers Area, and is updated regularly, keeping up to date with latest advice. Such links include Safer NEL, O2 and NSPCC Net Aware Campaign 'Guide to the Social Networks your children use' and more.

11: Identifying, reporting and responding to inappropriate use

The receipt of any communication that makes a person feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature, must be immediately reported to a member of staff. The recipient must not respond to any such communication. Any digital communication between staff and pupils or parents / carers (email, chat, etc) must be professional in tone and content. These communications may only take place on official school systems. Personal email addresses, text messaging or social media must not be used for these communications (see Media Policy).

12: Adjoining Policies

ICT Acceptable Use
Please see Best Futures ICT Acceptable Use Policy, which explains in more details the rules we follow as a school to keep everyone safe on the internet.

Media Policy
Best Futures Media Policy explains how information may be shared on and offline. Our Media Policy also includes Data Sharing Protocol.

Child Protection and Safeguarding
Includes information on Radicalisation and Extremism, Child Sexual Exploitation and Child Criminal Exploitation, Peer on Peer abuse (including Sexting and Up skirting) Social Media, Online Safety and more.

Code of Conduct
Staff Code of Conduct includes information on acceptable forms of Internet Use including Emails and sharing documents.

13: Helpful websites / Links to further information

Keeping Children Safe in Education
Keeping children safe in education - GOV.UK

Working Together to Safeguard Children
Working together to safeguard children - GOV.UK

Safer NEL SaferNEL | Staying safe online - SaferNEL

Internet Matters https://www.internetmatters.org/

Keeping Children Safe Online NSPCC https://www.nspcc.org.uk/keeping-children-safe/online-safety/

Google Be Internet Legends https://beinternetlegends.withgoogle.com/en_uk

Parent Zone https://www.parents.parentzone.org.uk/

Reporting Harmful Content https://reportharmfulcontent.com/?lang=en

Educate Against Hate https://educateagainsthate.com/

Common Sense Media https://www.commonsensemedia.org/

Think U Know https://www.thinkuknow.co.uk/

This list is not exhaustive.

Executive Principal:	Dawn Best	Signature	D H Best	**Date:**	25.04.25
CIC Board member for Safe-guarding:	Jenny Kinnaird	Signature	J A Kinnaird	**Date:**	15.05.23
DSL:	Kara Bradley	Signature	K.Bradley	**Date:**	15/05/2023