BEECHWOOD
Primary School

E-SAFETY

JANUARY 2023
Spring Term

Approved by: **Engagement & Wellbeing Committee** Date:

Last reviewed on: **January 2023**

Next review due by: **January 2025**

E-SAFETY POLICY

1.Rationale:

E-Safety encompasses the use of new technologies that are used by children and young adults throughout society. These technologies include websites, learning platforms, e-mail and instant messaging, chat rooms and social networking, mobile devices and music and game downloading. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

At Beechwood, we teach e-safety to ensure children recognise risks and are able to behave appropriately to keep themselves and others safe and legal. We educate children to ensure they understand all aspects of e-safety both in and out of the classroom.

E-Safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and pupils; encouraged by education and made explicit through published policies.
- Sound implementation of e-safety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband from an approved Internet Service Provider using suitable filtering.
- National Education Network standards and specifications.

2. E-safety Leadership:

Beechwood's lead on e-safety is David Francis. He co-ordinates e-safety assisted by the Learning and Outcomes Core Strand.

The E-Safety policy builds on the Cheshire e-Safety policy and government guidance. Its implementation is reviewed biennially.

3. Roles and Responsibilities:

Senior Leadership Team (SLT)

The SLT will be responsible for:

- Ensuring the safety (including e-safety) of all members within the Beechwood community;
- Ensuring that staff receive suitable CPD;
- Knowing the procedures to follow in the event of a serious allegation being made against a member of staff.

E-Safety Lead

The e-safety lead will be responsible for:

- Ensuring that all staff are aware of how to deal with e-safety incidents;
- Provide advice and training for staff;
- Attending appropriate meetings and courses;
- Providing training for the DSL and members of the safeguarding council;
- Reporting to SLT and Governors where appropriate.

Staff

All staff will be responsible for:

- Increasing their awareness of how to safeguard children within the context of e-safety;

- Regularly carrying out e-safety activities with the children, across all subjects and particularly at the start of computing lessons;
- Monitoring ICT activity in lessons, especially in KS2 with the introduction of Showbie and individual electronic devices;
- Being vigilant for e-safety issues in relation to digital cameras, mobile phones etc.

Pupils

Pupils will be responsible for:

- Ensuring that they use the ICT systems in school by following the Pupil Acceptable Use Policy. It is expected that this is signed when the child first enters Beechwood Primary School;
- Ensuring that they understand the importance of reporting abuse, misuse or inappropriate materials and that they know how to do this.

Parents and Carers

Parents and Carers will be responsible for:

- Endorsing (by signature) the Pupil Acceptable Use Policy (when their child enters the school);
- Making a decision as to whether they consent for their child to be included in photographs, as well as the photographs being used in the public domain (e.g. on the school website/school Facebook and/or Twitter).

4. Teaching and Learning:

The purpose of internet use at Beechwood Primary is to raise educational standards, promote achievement, support the professional work of staff and enhance the school's management information, business and administration systems.
Internet use is a part of the statutory curriculum and a necessary use for staff and pupils.

The internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality internet access as part of their learning experience.

Pupils use the internet outside of school and will learn how to evaluate internet information to take care of their own safety and security.

Internet - Enhance Learning

Internet access will be planned to enrich and extend learning activities.
The school internet access will be designed expressly for pupil and family use and will include filtering appropriate to the age of pupils.

Pupils and families will be taught what internet use is acceptable and what is not and given clear objectives for internet use.

Pupils will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.

Internet - Evaluating Content

If staff or pupils discover unsuitable sites, the URL, time, date and content will be reported to the e-safety lead.

The school will ensure that the use of internet derived materials by staff and pupils complies with copyright law.

Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy. This is explicitly taught as part of the computing curriculum in KS2.

5. Published Content and the School Website:
The contact details on the website are the school address, e-mail and telephone number. Staff or pupils' personal information will not be published. The headteacher will take overall editorial responsibility and ensure that content is accurate, appropriate and regularly updated.

Photographs that include pupils will be selected carefully. Pupils' full names will not be used on the website in association with photographs.

Consent from parents or carers will be obtained before photographs of pupils are published on the school website and on the school Facebook page and/or Twitter (this is included in the induction pack).

6. Social Networking and Personal Publishing:
The school will block/filter access to social networking sites. Pupils will be advised never to give out personal details of any kind which may identify them or their location. Pupils and parents may be advised that the use of social network spaces outside school is inappropriate for primary aged pupils. Staff are advised that they should consider the consequences and possible repercussions of any information that they make available online, for example on a social networking site. Particular care should be taken in the posting of photographs, videos and information related to the school, school life, staff and pupils.

7. Extremism and Radicalisation:
The school takes extremism and radicalisation very seriously and will ensure that all staff and governors have received the appropriate DFE 'Prevent' training. All staff will follow the policy guidelines and understand the need to be vigilant around school. Children are taught about dangers of radicalisation and extremist views as appropriate to their age and development.

8. Managing Filtering:
The school will work with the Cheshire East Council, DFE and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved. If staff or pupils discover an unsuitable site, it must be reported to the e-Safety Lead who should be known to all members of the school community. Staff will work alongside Cheshire East Council to ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

9. Managing Emerging Technologies:
Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed. Staff mobile phones will not be used during lessons or formal school time. They will be kept in bags/desk drawers and/or cupboards and only used in areas completely away from pupils e.g. side offices and the staffroom. Pupils who bring a mobile phone to school will hand it in to their class teacher/teaching assistant as soon as they come into school. These will be handed back at the end of the school day.

The sending of abusive or inappropriate text messages is forbidden. Staff will not use personal equipment or non-school personal electronic accounts when contacting students. They will be issued with a school phone where contact with pupils is required.

10. Protecting Personal Data:
Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018.

Please see the Data Protection policy.

11. Assessing Risks:
The school will take all reasonable precautions to ensure that users access only appropriate 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 school computer or ipad. Neither the school nor the Local Authority can accept liability for the material accessed, or any consequences of internet access. The school will regularly audit ICT provision to establish if the e-safety policy is adequate and that its implementation is effective.

12. Handling E-safety Complaints:
Complaints of internet misuse will be dealt with by a senior member of staff. Any complaint about staff misuse must be referred to the Headteacher. Complaints of a child protection nature must be dealt with in accordance with school's safeguarding and child protection policy and procedures.

Please see the Safeguarding & Child Protection policy.

13. Introducing the Policy to Stakeholders:
Pupils **-** E-safety rules will be posted in all classrooms and discussed with the pupils at the start of each year. Pupils will be informed that network and internet use will be monitored. An e-safety assembly for Years 3 - 6, led by the e-safety Lead, will take place at least annually to remind children of appropriate uses.

Staff **-** All staff will be requested to read and sign for to say they have understood the school e-Safety policy at the first INSET day in September. Its importance will be explained. Staff should be aware that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential. The School Business Manager (SBM) will regularly monitor internet use and the sites being accessed. Where sites are not appropriate to the job role, staff may be subject to disciplinary procedures.

Parents – Links to the e-safety policy are available on the school website. Each year an assembly and workshops on e-safety will be provided for parents and carers in line with Internet Safety Day.

14. Remote Learning
For the purposes of remote learning, children have been issued a school email address which can only be used as part of the Beechwood group to access any virtual lessons. A secure platform for live lessons will be used if required and only Beechwood staff will be able to allow access.

Any welfare calls to children may need to be made by staff working from home. Where a personal phone needs to be to be used, staff will be asked to block their personal number first.

E-SAFETY POLICY

This policy was adopted at a meeting of the Engagement and Wellbeing Governor sub-committee, held on: ______________________________

Date to be reviewed: **January 2025**

Signed:

Name of signatory :	Sara Harper	J. Cargill
Role of signatory:	Headteacher	Chair of Governors