E-Safety Policy

Keeping Pupils Safe Online

Date of Completion: February 2023
Date of Next Review: January 2025
Governor Approved: 29.03.2023

Version 2.0

1. Purpose

The purpose of this policy is to describe the safeguarding measures in place for adults and children in school:

- the ground rules for using the Internet and online technologies
- how these fit into the wider context of our other school policies
- the methods used to protect children from unsuitable content

At Longthorpe Primary School, we feel that the most successful approach lies in a combination of site filtering, of supervision and by fostering a responsible attitude in our pupils in partnership with parents and carers.

2. Rationale

At Longthorpe Primary school we believe that the use of technologies in school brings great benefits and can be used to raise standards and achievement. To live, learn and work successfully in an increasingly complex and information-rich society, our children must be able to use technology effectively. Use of ICT can at the same time present risks, which need to be contained.

Some of the dangers internet users may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

Although the risk cannot be completely eliminated it is essential, through good educational provision to manage the risk and deal with any threat to safety.

3. Teaching and Learning Using Online Technologies

Longthorpe Primary School recognises that different users will be expected to use the school's technology systems in different ways – appropriate to their age or role in school. We correspond the e-safety lessons taught with the children's ages and understanding of the internet in the wider world.

When using online technologies, it is essential that children understand how to behave in a safe and responsible manner and also how to react when faced with inappropriate content or situations which make them feel uncomfortable. At Longthorpe Primary School we believe that a comprehensive programme of e-safety education is vital for developing our pupils' ability to use technologies safely.

E-safety is taught from the day children arrive at Longthorpe and is a curriculum area studied regularly from EYFS through to Year 6. This is achieved using the Keeping Safe Curriculum which is taught each week. Children are taught how to stay safe, how to protect their personal information and how to deal with inappropriate and uncomfortable situations which may arise. Members of staff constantly monitor pupils' use of the internet and other technologies and can monitor pupils' use of communication and publishing tools.

Parents are provided resources via the school website and email to empower them to help keep their children safe whilst on the internet. The school does not provide ICT support to parents in relation to home security settings but instead will signpost them to information about control mechanisms on personal devices.

4. Technology in our School

Combined with internal procedures, the school's ICT infrastructure is designed to minimise the risks associated with adult and pupil use of technology.

The School's Internet Service Provider, E2BN provides a filtering system aimed at schools and academies. This helps to ensure that staff and pupils rarely encounter material which is inappropriate or offensive. In addition to this, the internal firewall also allows additional filtering to be applied if required.

The school's network can either be accessed using a physical or wireless connection. All wireless networks are password secured. Guest or visitor internet access and staff personal devices can only access the internet through specific wireless networks.

The School operates monitoring software in school for domain computers that report against blacklisted words to help identify potential issues. Each month this is reviewed to identify any misuse of technological resources or safeguarding concerns.

All pupils (except EYFS) and staff have individual, password protected logins to the school network. All online accounts are also password protected and are configured to provide security and prevent misuse wherever possible.

School iPad devices are configured via a Mobile Device Management (MDM) solution that allows the Trust and School centralised control over the settings and deployment of applications.

5. Reporting and Responding to Incidents

It is important that all staff are aware of how to respond if an e-safety incident occurs or they suspect a child is at risk through their use of technology. Responding to an e-safety incident in school is no different to responding to other incidents in school.

Any technology/account breaches or incidents should immediately be reported to both the ICT Subject Lead and ICT Manager for an appropriate response. Breaches of personal data are dealt with in line with the Trust's GDPR policy.

Any poor behaviour related incidents (e.g. online bullying) can be reported to a member of the senior leadership team.

Any safeguarding concerns or incidents should immediately be reported to one the schools designated Safeguarding officers in line with the School's safeguarding procedures.

Step 1: Identify who is involved
Step 2: Establish the kind of activity involved and whether it is illegal or inappropriate.
Step 3: Ensure that the incident is documented using the standard child protection incident logging form (see appendix)

If the incident involves or leads to an allegation against a member of staff, the school will follow the usual procedures for dealing with any allegation against a member of staff

If an e-safety incident occurs Longthorpe Primary will follow its usual procedures for dealing with other incidents including internal sanctions and involvement of parents (this may include the deactivation of accounts or restricted access to systems as per the school's Acceptable Use Policy).

This Policy is to be Read in Conjunction with:-

- GDPR Policy
- Child Protection & Safeguarding Policy
- Acceptable Use Policy
- Anti-Bullying Policy
- Behaviour Policy
- Computing & ICT Policy