Digital Resilience Policy

Reviewed on 10.23
To be approved by Full Governing Body in 11.23

The Acceptable Use of the Internet and related Technologies

Contents

Overview
Managing the Internet safely
Managing e-mail safely
Using digital images and video safely
Using the school network, equipment and data safely
Infringements and possible sanctions

Our e-Safety Policy has been written by the school, building on the Northern Grid for Learning (LGFL) exemplar policy and BECTA guidance. It has been agreed by the senior management and approved by Governors. It will be reviewed annually.

Context

Transforming learning and children's services have set out the government plans for taking a strategic approach to the future development of Computing.

"The Internet and related technologies are powerful tools, which open up new prospects for communication and collaboration. Education is embracing these new technologies as they bring with them fresh opportunities for both teachers and learners.

To use these technologies effectively requires an awareness of the benefits and risks, the development of new skills, and an understanding of their appropriate and effective use both in and outside of the classroom." DfES, eStrategy 2005

Children and young people are:

• safe from maltreatment, neglect, violence and sexual exploitation
• safe from accidental injury and death
• safe from bullying and discrimination

- have the knowledge and understanding of what safeguarding is.
  • safe from crime and anti-social behaviour in and out of school
  • secure, stable and cared for.

Much of these aims apply equally to the 'virtual world' that children and young people will encounter whenever they use computing in its various forms. For example, we know that the internet has been used for grooming children and young people with the ultimate aim of exploiting them sexually; we know that computing can offer new weapons for bullies, who may torment their victims via websites or text messages; and we know that children and young people have been exposed to inappropriate content when online, which can sometimes lead to their involvement in crime and anti-social behaviour.

It is the duty of the school to ensure that every child in their care is safe, and the same principles should apply to the 'virtual' or digital world as would be applied to the school's physical buildings.

This Policy document is drawn up to protect all parties – the students, the staff and the school and aims to provide clear advice and guidance on how to minimise risks and how to deal with any infringements.

1. The technologies

Computing the 21st Century has an all-encompassing role within the lives of children and adults. New technologies are enhancing communication and the sharing of information. Current and emerging technologies used in school and, more importantly in many cases, used outside of school by children include:

- Social networking applications and personal publishing tools could include, but are not limited to
- The internet
- E mail
- Social Networking (E.g. Facebook, Instagram, Snapchat)
- Messenger Apps (E.g. Facebook Messenger, Whatsapp, KIK, Viber)
- Video chat applications (E.g Skype, Omeagle, Yubo)
- Media sharing services (E.g. Musical.ly, You Tube, Vines)
- Micro-Blogging Applications (E.g. Twitter)
- Online discussion forums (E.g. Reddit, 4 Chan, IGN)
- Blogs (E.g. Blogger, Live Journal, Xanga)
- Music downloads
- Mobile phoned

2. Whole school approach to the safe use of computing
a safe computing environment includes three main elements at this school:

An effective range of technological tools;

Policies and procedures, with clear roles and responsibilities;

A comprehensive e-Safety education programme for pupils, staff and parents.

Reference: Becta – E-safety Developing whole-school policies to support effective practice

3. Roles and Responsibilities

E-Safety is recognised as an essential aspect of strategic leadership in this school and the Head, with the support of Governors, aims to embed safe practices into the culture of the school. The Headteacher ensures that the Policy is implemented and compliance with the Policy monitored. The responsibility for e-Safety has been designated to a member of the senior management team.

Our e-Safety Coordinator ensures they keep up to date with e-Safety issues and guidance through liaison with the Local Authority e-Safety Officer and through organisations such as BECTA and The Child Exploitation and Online Protection (CEOP) .

The school's e-Safety coordinator ensures the Head, senior management and Governors are updated as necessary.

Governors need to have an overview understanding of e-Safety issues and strategies at this school. We ensure our governors are aware of our local and national guidance on e-Safety and are updated at least annually on policy developments.

All teachers are responsible for promoting and supporting safe behaviours in their classrooms and following school e-Safety procedures. Central to this is fostering a 'No Blame' culture so pupils feel able to report any bullying, abuse or inappropriate materials.

Prevent is part of CONTEST, the Government's strategy to address terrorism. The main aim of Prevent is to stop people becoming terrorists or supporting terrorism. Prevent focuses on all forms of terrorist threats. E.g. international terrorism, far right extremists (among others).
The Government's Prevent strategy can be found at the following address:
www.homeoffice.gov.uk

Three key themes

- Safeguarding vulnerable individuals through the provision of advice and support and intervention projects.
- Working closely with institutions such as Universities, Schools, Prisons, Health, Charities and faith establishments.
- Challenging terrorist ideology by working closely with other local and national agencies, partners and our communities

These refer to Keeping Children Safe in Education 2020

The use of technology has become a significant component of many safeguarding issues. Child sexual exploitation; radicalisation; sexual predation: technology often provides the platform that facilitates harm. An effective approach to online safety empowers a school or college to protect and educate the whole school or college community in their use of technology and establishes mechanisms to identify, intervene in, and escalate any incident where appropriate.

The breadth of issues classified within online safety is considerable, but can be categorised into three areas of risk:

• **content**: being exposed to illegal, inappropriate or harmful material; for example pornography, fake news, racist or radical and extremist views;

• **contact:** being subjected to harmful online interaction with other users; for example commercial advertising as well as adults posing as children or young adults; and

• **conduct**: personal online behaviour that increases the likelihood of, or causes, harm; for example making, sending and receiving explicit images, or online bullying.

All staff should be familiar with the schools' Policy including:

• Safe use of e-mail;
• Safe use of Internet including use of internet-based communication services, such as instant messaging and social network;
• Safe use of school network, equipment and data;
• Safe use of digital images and digital technologies, such as mobile phones and digital cameras;
• publication of pupil information/photographs and use of website;
• eBullying / Cyberbullying procedures;
• their role in providing e-Safety education for pupils;

Staff are reminded / updated about e-Safety matters at least once a year.

4. How will complaints regarding e-Safety be handled?

The school will take all reasonable precautions to ensure e-Safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the school nor the Local Authority can accept liability for material accessed, or any consequences of Internet access.

Staff and pupils are given information about infringements in use and possible sanctions. Sanctions available include:
• interview/counseling by tutor / teacher / e-Safety Coordinator / Headteacher;
• informing parents or carers;
• removal of Internet or computer access for a period, [which could ultimately prevent access to files held on the system, including examination coursework];
• referral to LA / Police.

Our e-Safety Coordinator acts as first point of contact for any complaint. Any complaint about staff misuse is referred to the Headteacher.

Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with school / LA child protection procedures.

Staff must be aware that Tier restrictions means children are at home more than they have ever been. Children are using technology more than ever. Statistically this means children are a greater risk on line.