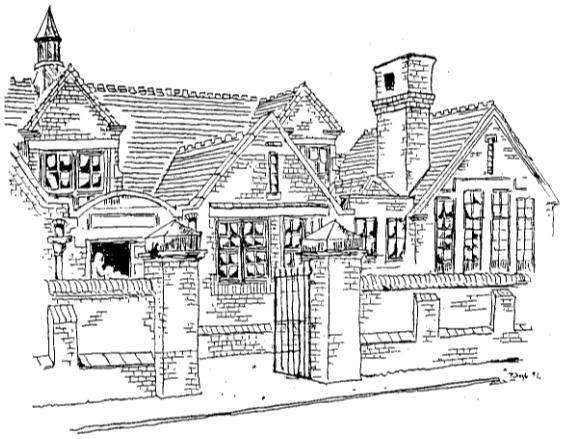
Netherfield Primary School

E-Safety Policy

December 2016



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

This e-Safety Policy has been approved by the Headteacher, SMT and Governors. It will be reviewed annually.

Created by:	Vicky Buckland
Date:	5th December 2016
To be revised:	25th July 2017

Rationale

The Purpose of the New Computing Curriculum: A high-quality computing education equips pupils to use computational thinking and creativity to understand and change the world. Computing also ensures that pupils become digitally literate – able to use, and express themselves and develop their ideas through, information and communication technology – at a level suitable for the future workplace and as active participants in a digital world. Pupils must be taught to use technology safely, respectfully and responsibly; recognise acceptable/unacceptable behaviour; identify a range of ways to report concerns about content and contact.
(Available from:https://www.gov.uk/government/publications/national-curriculum-in-england-computing-programmes-of-study/national-curriculum-in-england-computing-programmes-of-study)

Harnessing Technology: *Transforming learning and children's services*[1] sets out the government plans for taking a strategic approach to the future development of ICT.

"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 the classroom." DfES, e Strategy 2005

The Green Paper E*very Child Matters*[2] and the provisions of the *Children Act 2004*[3]*, Working Together to Safeguard Children*[4] sets out how organisations and individuals should work together to safeguard and promote the welfare of children.

The 'staying safe' outcome includes aims that children and young people are:

- Safe from maltreatment, neglect, violence and sexual exploitation
- Safe from accidental injury and death
- Safe from bullying and discrimination
- Safe from crime and anti-social behaviour in and out of school
- Secure, stable and cared for.

Technology offers unimaginable opportunities and is constantly evolving. Access is currently becoming universal and increasingly more mobile, and pupils are using technology at an ever earlier age (http://www.e2bn.org/esafety/399/e-safety-and-ofsted.html -Revised E-safety Briefing April 2014)
Much of these aims apply equally to the 'virtual world' that children and young people will encounter whenever they use ICT 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 ICT 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

[1] http://www.dfes.gov.uk/publications/e-strategy/
[2] See children act 2004 (http://www.opsi.gov.uk/acts/acts2004/20040031.htm)
[3] See Every Child Matters website (http://www.everychildmatters.gov.uk)
[4] See Working Together to Safeguard Children: A guide to inter-agency working to safeguard and promote the welfare of children. See Every Child Matters website (http://www.everychildmatters.gov.uk/_files/AE53C8F9D7AEB1B23E403514A6C1B17D.pdf)

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.

The Keeping Children Safe in Education document states that '***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 and escalate any incident where appropriate.'***
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/550511/Keeping_children_safe_in_education.pdf

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

1. The technologies

ICT in 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:

- The Internet
- E-mail
- Instant messaging (msn/skype) often using simple web cams
- Blogs (an on-line interactive diary)
- Podcasting (radio/audio broadcasts downloaded to computer or MP3/4 player)
- Social networking sites (facebook/snapchat)
- Video broadcasting sites (youtube/iplayer/4OD)
- Chat rooms (teenchatl)
- Gaming sites (neopets/miniclip.com/runescape)
- Music download sites (itunes)
- Mobile phones with camera and video functionality
- Smart phones with e-mail, web functionality and cut down 'office' applications
- Games Consoles (xbox, playstation360, Nintendo Wii)

2. Whole school approach to the safe use of Computing

Creating a safe Computing learning environment include three main elements at this school:

- An effective range of technological tools – laptops, iPads, Flip cameras, cameras
- Policies and procedures, with clear roles and responsibilities;
- A comprehensive e-safety education programme for pupils, staff and parents.

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 head teacher ensures that the Policy is implemented and compliance with the Policy monitored. The responsibility for e-safety has been designated to all staff with the Computing co-ordinator overseeing it is being followed and used.

Our school e-safety Co-ordinator is Vicky Buckland. 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 Protections (CEOP)[5]. The school's e-safety coordinator ensures the Head, senior management and Governors are updated as necessary.

Governors need to have and overview understanding of e-safety issues and strategies at this school. We ensure our governors are aware of our local and national guidance[6] 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.

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.

[5] http://www.ceop.gov.uk/
[6] Safety and ICT- available from Becta at http://schools.becta.org.uk

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 e-Safety Coordinator / Deputy Headteacher/ 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]
- 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.

5. Special Educational Needs:

SEN children to be able to access ICT equipment as needed, to help and support them with their learning and ensure progression is made.