



## Policy: E -Safety

<b>Name of School</b>	<b>Holy Trinity Church of England School East Finchley</b>
<b>School E-Safety Co-ordinator</b>	<b>Mrs Androulla Christou</b>
<b>Policy review Date</b>	<b>January 2016</b>
<b>Date of next Review</b>	<b>January 2017</b>
<b>Who reviewed this policy?</b>	<b>Mrs Androulla Christou</b>
<b>Approved by Governing Body</b> (signature and date)	

Our e-Safety Policy has been written by the school, building on the London 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.

# **Policy: E –Safety Contents**

<b>Section 1</b>	<b>Overview - The Acceptable Use of the Internet and related Technologies</b>
<b>Section 2</b>	<b>Policy - Managing the Internet safely</b>
<b>Section 3</b>	<b>Policy – Managing email</b>
<b>Section 4</b>	<b>Policy – Use of digital and video images</b>
<b>Section 5</b>	<b>Policy – Managing equipment</b>
<b>Section 6</b>	<b>Policy – How will Infringements be handled</b>

## **Summary Policy Statements**

These are taken from sections 2 - 6 for you to customise, and should be distributed to staff for day to day reference.

### ***Further separate documents:***

The Acceptable Use Agreements (AUA) should be signed and retained.

AUA (Acceptable Use Agreement) – Parents

AUA – Pupils

AUA – Staff

### **Guidance:**

Safeguarding and protecting children

Cyberbullying

What do we do if? (Checklist for staff)

### **Resource :**

12 Rules for Responsible ICT use

## **Section 1 Overview : The Acceptable Use of the Internet and related Technologies**

- a. **Context**
- b. **The Technologies**
- c. **Whole school approach to safe use of ICT**
- d. **Roles and responsibilities**
- e. **Communications**
- f. **How will complaints regarding e-safety be handled**

### **a. Context:**

**Ofsted (2009)** : A good school 'integrates issues about safety and safeguarding into the curriculum so that pupils have a strong understanding of how to keep themselves safe. The school is pro-active in building on collaborative working with other key agencies to reduce the risk of harm to pupils.'

### **A school is inadequate if:**

'Safeguarding regulations and duties are not met.

or Arrangements for safeguarding are not robust and there is no system to maintain and update them, or the systems that are in place are ineffective.

or Pupils do not receive sufficient information, or support, to enable them to keep themselves safe.

or There is little or unproductive involvement of key agencies.

*If the school is judged to be inadequate in this strand of the evaluation schedule, its overall effectiveness is likely to be judged to be inadequate'*

*Ofsted's evaluation schedule of judgements for schools inspected under section five of the Education Act 2005, from September 2009 P age 51*

### **References in the SEF**

**A2.5** The extent to which pupils feel safe

**A4.7** The effectiveness of safeguarding procedures

### **SRF elements – working towards ICT Mark**

#### **1c-4 Safeguarding**

The school is aware of its responsibilities in ensuring that ICT usage by all network users is responsible, safe and secure.

There are relevant and comprehensive policies in place which are understood and adhered to by many network users.

#### **3b-2 Effective and safe use of digital resources**

Most pupils have a good range of skills that enable them to access and make effective use of digital resources to support their learning. They understand the issues relating to safe and responsible use of ICT and adopt appropriate practices

*Harnessing Technology: Transforming learning and children's services*<sup>1</sup> 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 of the classroom."*  
DfES, eStrategy 2005

The Green Paper *Every Child Matters*<sup>2</sup> and the provisions of the *Children Act 2004*<sup>3</sup>, *Working Together to Safeguard Children*<sup>4</sup> 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.

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.

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.

## **b. The technologies**

ICT in the 21<sup>st</sup> 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:

---

<sup>1</sup> <http://www.dfes.gov.uk/publications/e-strategy/>

<sup>2</sup> See The Children Act 2004 [<http://www.opsi.gov.uk/acts/acts2004/20040031.htm>]

<sup>3</sup> See Every Child Matters website [<http://www.everychildmatters.gov.uk>]

<sup>4</sup> Full title: 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](http://www.everychildmatters.gov.uk/_files/AE53C8F9D7AEB1B23E403514A6C1B17D.pdf)]

- The Internet
- e-mail
- Instant messaging (<http://www.msn.com>, <http://info.aol.co.uk/aim/>) 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
- Video broadcasting sites (Popular: <http://www.youtube.com/>)
- Chat Rooms (Popular [www.teenchat.com](http://www.teenchat.com), [www.habbohotel.co.uk](http://www.habbohotel.co.uk))
- Gaming Sites (Popular [www.neopets.com](http://www.neopets.com), <http://www.miniclip.com/games/en/>, <http://www.runescape.com/> / <http://www.clubpenguin.com>)
- Music download sites (Popular <http://www.apple.com/itunes/> <http://www.napster.co.uk/> <http://www.kazaa.com/>, <http://www.livewire.com/>)
- Mobile phones with camera and video functionality
- Mobile technology (e.g. games consoles) that are 'internet ready'.
- Smart phones with e-mail, web functionality and cut down 'Office' applications.

### c. Whole school approach to the safe use of ICT

Creating a safe ICT learning 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.

*Ref: Becta - E-safety Developing whole-school policies to support effective practice*<sup>5</sup>

### d. 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 school **e-Safety Co-ordinator** is Androulla Christou

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)<sup>6</sup>. The school's e-Safety coordinator ensures the Head, senior management and Governors are updated as necessary.

<sup>5</sup> <http://schools.becta.org.uk/index.php?section=is>

<sup>6</sup> <http://www.ceop.gov.uk/>

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<sup>7</sup> 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.

Schools should include e-safety in the curriculum and ensure that every pupil has been educated about safe and responsible use. Pupils need to know how to contrail and minimise online risks and how to report a problem.

Schools should ensure that they make efforts to engage with parents over e-safety matters and that parents/guardians/carers have signed and returned an e-safety/AUP form.

## **e. Communications**

### **How will the policy be introduced to pupils?**

**Discussion:** Many pupils are very familiar with the culture of new technologies, they can be involved them in designing the School e-Safety Policy, possibly through a student council. Pupils' perceptions of the risks may not be mature; the e-safety rules will need to be explained or discussed.

E-safety should be taught in all year groups, covering age-appropriate issues. Useful e-safety programmes include:

- Barnet and LGfL e-Safety and e-literacy Framework for EYFS-Y6 ([www.safety.lgfl.net](http://www.safety.lgfl.net) )
- Think U Know; currently available for secondary pupils. ([www.thinkuknow.co.uk/](http://www.thinkuknow.co.uk/))
- Grid Club [www.gridclub.com](http://www.gridclub.com)
- The BBC's ChatGuide: [www.bbc.co.uk/chatguide/](http://www.bbc.co.uk/chatguide/)

Possible statements:

- An e-safety training programme will be introduced to raise the awareness and

---

<sup>7</sup> Safety and ICT - available from Becta, the Government agency at:  
[http://schools.becta.org.uk/index.php?section=lv&catcode=ss\\_lv\\_str\\_02&rid=10247](http://schools.becta.org.uk/index.php?section=lv&catcode=ss_lv_str_02&rid=10247)

importance of safe and responsible internet use.

- Instruction in responsible and safe use should precede Internet access.
- An e-safety module will be included in the PSHE, Citizenship or ICT programmes covering both school and home use.

### **How will the policy be discussed with staff?**

**Discussion:** It is important that all staff feel confident to use new technologies in teaching. Staff should be given opportunities to discuss the issues and develop appropriate teaching strategies

Staff must understand that the rules for information systems misuse. If a member of staff is concerned about any aspect of their ICT use in school, they should discuss this with their line manager to avoid any possible misunderstanding.

ICT use is widespread and all staff including administration, caretaker, governors and helpers should be included in appropriate awareness raising and training. Induction of new staff should include a discussion of the school's e-Safety Policy.

Possible statements:

- Staff should be aware that Internet traffic is monitored and can be traced to the individual user. Discretion and professional conduct is essential.
- Staff that manage filtering systems or monitor ICT use will be supervised by senior management and have clear procedures for reporting issues.
- Staff training in safe and responsible Internet use and on the school eSafety Policy will be provided as required.

### **How will parents' support be enlisted?**

**Discussion:** Internet use in pupils' homes is increasing rapidly. Unless parents are aware of the dangers, pupils may have unrestricted access to the Internet. The school may be able to help parents plan appropriate supervised use of the Internet at home.

Possible statements:

- Internet issues will be handled sensitively, and parents will be advised accordingly.
- A partnership approach with parents will be encouraged. This could include parent evenings with demonstrations and suggestions for safe home Internet use.
- Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be made available to parents.

### **f. 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/counselling by tutor / Head of Year / 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 Barnet 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 and Barnet LA child protection procedures.