Barnabas Oley School

E-Safety Policy

Version:	2.2		
Reviewed:	October 2018		
Approved:	S Reardon (Curriculum Chair)	Date:	October 2018

Revision History

Version	Author	Summary	Review Date	Next Review
1.00	E Makower		29/01/2009	Jan 2010
1.01	Curr Cmtee		09/03/2010	Mar 2011
2.0	B Smith/SMT	Complete overhaul with guidance from The ICT Service (LA)	Jun 2014	Oct 2016
2.1	Curr Cmtee	Minor amendments	Nov 2016	Oct 2018
2.2	Curriculum Committee	Minor amendments	Oct 2018	Oct 2020

Contents

1 Introduction 1

2 The Background to this Policy 1

3 Rationale 1

4 Responsibilities 2

5 Teaching and Learning Using Online Technologies 3

6 Technology in School 4

7 The E-Safety Curriculum 4

8 Safeguarding Children Online 5

9 Responding to Incidents 5

10 Dealing with Incidents and Seeking Help 5

11 Terms Used in this Policy 6

12 Cross Referencing Documents 6

Appendices

A. Acceptable Use Policy – Pupils 9

B. Acceptable Use Policy - Staff 10

Blank Page

1 Introduction

Barnabas Oley Church of England Primary School believes that the use of information and communication technologies not only creates opportunities for our children but brings great benefits to their lives as well. However, with these opportunities are a number of associated risks. We need to recognise the safeguarding issues and use this policy to plan to minimise the risks accordingly.

E-Safety in schools is a child safety and not an ICT issue. Therefore, this policy should be viewed alongside other Safeguarding policies including those for behaviour, anti-bullying, personal, social and health education (PSHE), citizenship and safeguarding and Child Protection (KCSIE 2018).

2 The Background to this Policy

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

- the ground rules we have developed in school 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 sites containing pornography, racist or politically extreme views and violence.

Ultimately, the responsibility for setting and conveying the standards that children are expected to follow when using technology, media and information resources, is one the school shares with parents and carers. At Barnabas Oley CoE 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.

The development of our safety policy involved:

Headteacher:	Mrs Michelle Downes
Senior Leaders:	Miss Claire Jarvis
ICT Subject Leaders:	Mrs Josephine Hussey
Governors:	Curriculum Committee
Parents and Carers	

It will be available on the school website and by request from the school office.

3 Rationale

At Barnabas Oley CoE School, we believe that the use of information and communication technologies in schools brings great benefits. To live, learn and work successfully in an increasingly complex and information-rich society, our children must be able to use technology effectively.

The use of these exciting and innovative technology tools in school and at home has been shown to raise educational standards and promote pupil achievement. Yet at the same time we recognise that the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they 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.

While children and young people need support to keep them safe online, the risks associated with the use of technology are not restricted to just them. E-Safety issues can also affect adults who work or are associated with the school. For example, school and personal data being entered on web/social networking sites, fraudulent email traps and cyberbullying. It is impossible to eliminate risk completely. It is therefore essential, through good educational provision to manage the risk and deal with any threat to safety.

4 Responsibilities

4.1 Teaching and Support Staff are responsible for ensuring that:

- they have an up to date awareness of E-Safety matters and of the current school E-Safety policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy (AUP)
- they report any suspected misuse or problem to the Headteacher for investigation
- all digital communications with students, parents or carers should be on a professional level and only carried out using official school systems
- E-Safety issues are embedded in all aspects of the curriculum and other activities
- pupils understand and follow the E-Safety and acceptable use policies
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- in lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

4.2 Child Protection Designated Personnel

Designated personnel should be trained in E-Safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying

4.3 Pupils

- are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Policy
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying.
- should understand the importance of adopting good E-Safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school.

4.4 Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about national / local E-Safety campaigns / literature. Parents and carers will be encouraged to support the school in promoting good E-Safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website
- their children's personal devices in the school (where this is allowed)

5 Teaching and Learning Using Online Technologies

The internet is a part of everyday life for education, business and social interaction.

Benefits of using online technologies in education include:

- Access to world-wide educational resources
- Access to experts who would otherwise be unavailable
- Access to anytime, anywhere learning
- Collaboration across schools, networks of schools and services

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 Barnabas Oley CoE Primary School we believe that a comprehensive programme of E-Safety education is vital for developing our pupils' ability to use technologies safely. This is achieved using a combination of discrete and embedded activities drawn from a selection of appropriate materials.

We believe that just as children learn how to swim by going to a swimming pool so they will learn safe life-long online behaviours by accessing and using the internet. Members of staff constantly monitor pupils' use of the internet and other technologies and are able to monitor pupils' use of communication and publishing tools. Our programme for E-Safety education is evidenced in teachers' planning either as discrete or embedded activities.

Messages involving Risks and Rules and Responsibilities are taught and/or reinforced as detailed in the school's Acceptable Use Policies (see appendices).

6 Technology in School

The school's ICT infrastructure is designed to minimise the risks associated with adult and pupil use of technology. This is provided and maintained by both the East of England Broadband Network (E2BN) and the Local Authority's Education ICT Service.

> *E2BN's Protex web filtering system received full Becta (British Educational Communications and Technology Agency) accreditation in 2007 by blocking over 90% of all inappropriate material. E2BN also manage a distributed caching service which is integrated with the web filtering service.*
>
> *Ref: E2BN Website*

This helps to ensure that staff and pupils rarely encounter material which is inappropriate or offensive. If / when they do, the school's AUPs and E-Safety education programme ensure that they are equipped to deal with any issues in the most appropriate way.

Technologies regularly used by pupils and adult stakeholders include:

6.1 Staff:

- Laptops, desktops and iPads
- Cameras and video cameras, visualisers
- Internet, E-mail, central hosting including access to SIMS and confidential pupil information

6.2 Pupils:

- Laptops, desktops and iPads
- Cameras and video cameras, visualisers
- Internet, discussion forums, blogs and other communication tools
- Other peripherals such as programmable toys, dataloggers, control technology equipment

6.3 Others on school premises:

- Limited access to school systems such as filtered internet access using a visitor login.

Whilst we recognise the benefits of individual pupil logins to our school network, in KS1 we prefer to use year group logins for ease of access. As pupil move into KS2 they will then start to use individual logins. All members of staff have individual, password protected logins to the school network and visitors to the school can access part of the network using a generic visitor login and password. The school's network can either be accessed using a wired or wireless connection. However, the wireless network is encrypted to the standards advised by the Local Authority and the wireless key is kept securely by the school office. School pupils are not permitted to connect personal devices to the school's wireless network and the wireless key is only given to visitors to the school with permission from the Headteacher.

7 The E-Safety Curriculum

In line with recommendations in the E-Safety briefing for Ofsted Inspectors (Sept 2012) we have planned a range of age-related teaching and learning opportunities to help our pupils to become safe and responsible users of new technologies. These opportunities include:

- Specific activities throughout the year and Anti-bullying week (held traditionally in November)
- Age-relate classroom activities.

- Related work in PSHE lessons
- Posters and reminders in and around the school

8 Safeguarding Children Online

Our 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 acknowledge the need to:

Equip children to deal with exposure to harmful and inappropriate content and contact, and equip parents to help their children deal with these things and parent effectively around incidences of harmful and inappropriate conduct by their children.

UKCCIS (The UK Council for Child Internet Safety) – June 2008

The school has published Acceptable Use Policies for pupils and staff who sign to indicate their acceptance of our AUPs and relevant sanctions which will be applied should rules be broken. Please see appendices for full details.

Any known or suspicious online misuse or problem will be reported to the designated E-Safety Co-ordinator and/or Headteacher for investigation.

9 Responding to Incidents

It is important that all members of staff – teaching and non-teaching – 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. It is important that responses to E-Safety incidents are consistent with responses to other incidents in school. This may mean that serious actions have to be taken in some circumstances.

If an E-Safety incident occurs Barnabas Oley CoE Primary School will follow its agreed procedures for dealing with incidents including internal sanctions and involvement of parents (for ICT, this may include the deactivation of accounts or restricted access to systems as per the school's AUPs – see appendix). Where the school suspects that an incident may constitute a Child Protection issue, the usual Child Protection procedures will be followed.

10 Dealing with Incidents and Seeking Help

If a concern is raised, refer immediately to the Headteacher or designated personnel for child protection or, if necessary, the Chair of Governors.

It is their responsibility to:

Step 1: Identify who is involved – any combination of child victim, child instigator, staff victim, or staff instigator

Step 2: Establish the kind of activity involved and whether it is illegal or inappropriate. If in doubt they should consult the Education Child Protection Service helpline.

Step 3: Ensure that the incident is documented using the standard child protection incident logging form (see Safeguarding policy)

Depending on the judgements made at steps 1 and 2 the following actions should be taken:

Staff instigator – follow the standard procedures for Managing Allegations against a member of staff (see Whistle blowing policy). If unsure seek advice from the Local Authority Education Officer.

Staff victim – Seek advice from Educational personnel Management (EPM) and/or Educational Child Protection Service

Illegal activity involving a child – refer directly to Cambridgeshire Constabulary – 0845 456 4564 – make clear that it is a child protection issue

Inappropriate activity involving a child – follow standard child protection procedures. If unsure seek advice from Education Child Protection Service helpline.

Equally, if the incident involves or leads to an allegation against a member of staff, the school will follow the agreed procedures for dealing with any allegation against a member of staff (see Whistle blowing policy).

11 Terms Used in this Policy

AUP: Acceptable Use Policy. A document detailing the way in which new or emerging technologies may/may not be used – may also list sanctions for misuse.

Child: Where we use the term 'child' (or its derivatives), we mean 'child or young person'; that is anyone who has not yet reached their eighteenth birthday.

E-Safety: We use E-Safety, and related terms such as 'online', 'communication technologies', and 'digital technologies' to refer to all fixed and mobile technologies that children may encounter, now and in the future, which might pose E-Safety risks. We try to avoid using the term 'ICT' when talking about E-Safety as this implies that it is a technical issue – which is not the case. The primary focus of E-Safety is child protection: the issues should never be passed solely to technical staff to address.

PIES: A model for limiting E-Safety risks based on a combined approach to Policies, Infrastructure and Education, underpinned by Standards and inspection. Whilst not explicitly mentioned in this policy, this model provides the basis for this school's approach to E-Safety.

Safeguarding: Safeguarding is defined (for the purposes of this document) as the process of increasing resilience to risks when using technology through a combined approach to policies and procedures, infrastructure and education, underpinned by standards and inspection. E-Safety is just one aspect of a much wider safeguarding agenda within the UK, under the banner of Every Child Matters: Change for Children. Those with responsibility for the development and delivery of E-Safety policies should embed their work within the wider safeguarding agenda, and work across services to ensure that they are delivering the best possible opportunities for the children in their care.

Users: We use this term, and related terms such as service users and end users, to mean those people who will ultimately be bound by the provisions of an AUP. This might be pupils, staff, parents and carers, or members of the wider community.

12 Cross Referencing Documents

- Professional boundaries in relation to your personal internet use and social networking online – advice to staff (LSCB)
- Behaviour policy
- Safeguarding and Child Protection policy

- SRE (Sex and Relationships Education) policy
- Citizenship and PSHE policy
- Safer Working Practices policy
- Data Protection Policy
- County guidance (e.g. Use of Digital Images, e-mail)
- AUPs- staff, pupil, parents
- Anti-Bullying Policy
- School Complaints Procedure

Appendices

A. Acceptable Use Policy – Pupils

Rules for Responsible Internet Use - Pupils

The school has computers and iPads with Internet access to help our learning. These rules will help keep us safe and help us be fair to others.

Using the computers:

- I will not access other people's files;
- I will not bring in memory sticks or CD ROMS from outside school and try to use them on the school computers without prior permission.

Using the Internet:

- I will ask permission from a teacher before using the internet;
- I will report any unpleasant material to my teacher immediately because this will help protect other pupils and myself;
- I understand that the school may check my computer files and may monitor the Internet sites I visit;
- I will not complete and send forms without permission from my teacher;
- I will not give my full name, my home address or telephone number when completing forms.

Using e-mail:

- I will ask permission from a teacher before checking the e-mail;
- I will immediately report any unpleasant messages sent to me because this would help protect other pupils and myself;
- I understand that e-mail messages I receive or send may be read by others;
- The messages I send will be polite and responsible;
- I will only e-mail people my teacher has approved;
- I will only send e-mail when it has been checked by a teacher;
- I will not give my full name, my home address or telephone number;
- I will not use school e-mail facilities to arrange to meet someone outside school, hours

I have read and agree to the above rules for safe use of the internet;

Name:______________________________ Class: ___________________

Parent/Carer signature: _____________________________

Date: _________________________________

B. Acceptable Use Policy - Staff

The computer network and laptops and iPads are owned by the school, and may be used by children to further their education and by staff to enhance their professional activities including teaching, research, administration and management. The school's Internet Access Policy has been drawn up to protect all parties – the pupils, the staff and the school. The school reserves the right to examine or delete any files that may be held on its computer system or to monitor any internet sites visited.

Staff requesting Internet access should sign a copy of this Acceptable Internet Use Statement and return it to the Administration Officer.

- All internet activity should be appropriate to staff professional activity or the children's education;
- Access should only be made via the authorised account and password, which should not be made available to any other person;
- Users are responsible for all E-mail sent and for contacts made that may result in E-mail being received;
- Use for personal financial gain, gambling, political purposes or advertising is forbidden;
- Copyright of materials must be respected;
- Posting anonymous messages and forwarding chain letters is forbidden;
- As E-mail can be forwarded or inadvertently sent to the wrong person, the same professional levels of language and content should be applied as for letters or other media;
- Use of the network to access inappropriate materials such as pornographic, racist or offensive material is forbidden.

LAPTOPS/iPads/Tablets

- Staff need to be aware that laptops/iPads are insured if they are accidentally or maliciously stolen by means of forced entry or assault.
- If a laptop/iPad/ has been stolen the police need to be notified and a crime reference obtained.
- Staff need to be vigilant about where they store their laptop/iPad/ in school – it must not be left out on show at the end of the school day etc.
- Laptops/iPads/ will not be uncovered whilst in transit or left unattended in a vehicle.
- Laptops/iPads/ must only be connected to the internet at home through a firewall.

I agree to follow the guidelines for computer and Internet use as outlined above in the school's Internet Policy.

Name:

Signed: Date:

Authorised by: Mrs Michelle Downes, Headteacher Signed: Date: