Christ Church CE School
Online Safety Policy

Spring 2018

Christ Church
CE Primary School
Regents Park
NW1 4BD

Christ Church C of E Primary School
Online Safety Policy

CONTENTS

Christ Church C of E Primary School
Online Safety Policy

Mission Statement

The Christian Faith is at the heart of our school community. At Christ Church we care for each other and learn together.

Christ Church is a small, caring school which is committed to a broad, balanced curriculum and to a continual raising of standards. We aim to contribute to the spiritual, moral, cultural, mental and physical needs of every individual.

We are a Church of England school, with a strong commitment to the teaching of Christianity whilst supporting a multi-faith approach to the curriculum. We recognise, value and celebrate the rich cultural diversity that exists in our school.

The Christian ethos of the school is reflected in our positive, disciplined and calm atmosphere. We believe that effective learning takes place when children work in a purposeful and stimulating environment that supports a wide range of learning styles. Mutual respect between adults and children promotes excellent behaviour and well developed social skills. With this approach we seek to achieve high academic standards.

We aim to cater for each individual, taking particular account of any specific needs or abilities. We endeavour to ensure that all our children fulfil their potential and, within this context, we emphasise health and safety, enjoyment and achievement and the beginnings of responsibility for themselves and others. These skills will be carried forward to the next phase of education and throughout life.

The whole school community is committed to a collective responsibility for the implementation of the values inherent in this statement.

Our School Aims - **Every Child Matters**

The Ethos of the School

The school aims to provide a positive, disciplined, purposeful environment, within a Christian context. We aim to teach children to be caring, to exhibit good behaviour and appropriate social skills and to begin to take responsibility for themselves and others.

The Values of the School

The School aims to value every child and to contribute to the Spiritual, Moral, Cultural, Mental and Physical well being of our whole school community. We value the diversity of our community and we aim to promote the health and safety of everyone.

The Standards of the School

The School aims to teach a balanced Curriculum and to ensure that each child fulfils his or her potential. We aim to provide teaching and learning of a high standard. We believe that this is achieved when pupils are highly motivated, enjoy coming to school, and are appropriately challenged.

Christ Church C of E Primary School

Online Safety Policy

Date of policy: February 2018
Review date: February 2020

Introduction

- This policy is a statement of the aims and principles of promoting online safety at Christ Church Primary School.
- This policy will be submitted to the Governing Body. Review of the policy will take place once every two years.
- This policy replaces the Internet and E-mail policy to take into account the continuous developments in communication technology.
- This policy should be read in conjunction with the Information and Communications Technology (ICT) policy.

What is Online Safety?

- The School's online safety Policy replaces the Internet Policy to reflect the need to raise awareness of the safety issues associated with information systems and electronic communications as a whole.

- Online safety encompasses not only Internet technologies but also electronic communications such as mobile phones, iPads and wireless technology. It highlights the need to educate children and young people about the benefits, risks and responsibilities of using information technology. It provides safeguards and raises awareness to enable users to control their online experiences.

- The Internet is an unmanaged, open communications channel. The World Wide Web, e-mail, blogs and social networking all transmit information using the Internet's communication infrastructure internationally at low cost. Anyone can send messages, discuss ideas and publish material with little restriction. These features of the Internet make it an invaluable resource used by millions of people every day.

- Much of the material on the Internet is published for an adult audience and some is unsuitable for pupils. In addition, there is information on weapons, crime and racism, access to which would be more restricted elsewhere. Pupils must also learn that publishing personal information could compromise their security and that of others.

- Schools can help protect themselves by making it clear to pupils, staff and visitors that the use of school equipment for inappropriate reasons is "unauthorised". However, schools should be aware that a disclaimer is not sufficient to protect a school from a claim of personal injury and the school needs to ensure that all reasonable actions have been taken and measures put in place to protect users.

Rationale and Equal Opportunities

Why have an Online safety policy?

Our purposes in developing a policy to promote online safety are:

- To help children avoid the danger that new technologies such as the Internet – enabled mobile phones, iPads, social networking sites (such as MySpace and Facebook) and Instant messaging (IM) can occasionally bring.
- To educate children on the risks and responsibilities that go along with using such technologies.
- To support parents and carers in helping their children to stay safe when using information and communication technologies at home.
- To have procedures in place to deal with incidents of concern.
- To recognise the extra risks posed to children with special educational needs (SEN)
- To have a joint statement and explanation of our policy available for parents, governors and teachers.
- To protect themselves from legal challenge. The law is catching up with Internet developments: for example it is an offence to store images showing child abuse and to use e-mail, text or Instant messaging (IM) to 'groom' children. Such incidences of concern need to be dealt with appropriately.

Aims and Objectives for the Promotion of Online Safety

The overall aim of the promotion of online safety is to enable all children to be safe and responsible users of information and communication technologies, both in and out of school.

The aim is for children:

- to know how to use the Internet, iPads, e-mail, chatrooms, Instant messaging (IM), mobile telephones and other technologies safely and responsibly.
- to know that they can tell an adult if they have accessed or been subjected to inappropriate or offensive material via information and communication technologies.

The aim is for staff and other adults within the school:

- to be aware of the risks information and communication technologies, particularly new technologies, pose to children.
- to use the Internet, iPads, e-mail and other technologies safely within lessons, checking website content before using it with pupils.
- to use the Internet (including social networking sites), iPads, e-mail and other technologies responsibly during non-contact time at school.
- to be aware of the procedures in place should an incident of concern involving technology occur.

Online Safety in Teaching and Learning

Online safety can be taught in many curriculum areas.

Information and Communications Technology (ICT) and Computing

Online safety should be taught explicitly in 'Computing' lessons. In addition, children should be informed of the risks presented when introduced to a new form of technology, such as iPads and e-mail. Online safety may also be discussed in an ad hoc manner. For example, if children were using a website to play a number game and an advert for a gambling or dating site appeared, teachers could talk to children about whether they think they should click on that advert, what they think might happen if they do, if that advert is meant for children and so on.

Personal, Social and Health Education

Online safety should be taught as part of anti-bullying. Children need to learn that bullying via social networking sites, Instant messaging (IM), text messaging on mobile phones and e-mail is just as unacceptable as bullying face–to–face. It should be made clear that 'cyber bullying' (the name given to bullying via technology) is not acceptable at school or at home, and that children should approach adults for help if they are being bullied in any way. Cyber bullying should be dealt with in school just as other forms of bullying would be, with parental involvement where necessary.

Online safety should also be taught as part of 'stranger danger'. Children need to be aware that people they talk to online through Instant messaging (IM), social networking sites, e-mail and chatrooms may not be who they claim to be. Children must be taught NEVER to give out their personal details (such as their name, address, age and school) online, even if they think they know the person they are talking to.

The Foundation Stage

Many of the issues raised in this policy are not applicable to very young children in nursery and reception. However, these children can be taught basic safety skills. Teach children about 'stranger danger' and the importance of not speaking to adults they do not know. When using the Internet, teach children how to stay on one site.

Why Use Information and Communications Technology (ICT)?

Despite the potential risks, the use of information and communications technologies, particularly the Internet, is massively advantageous to children's learning. The teaching and learning of Computing and the use of the Internet is important because:

- Computing is a national curriculum subject (see ICT and Curriculum policy for teaching requirements.)
- Internet use is part of the Computing curriculum and a necessary tool for staff and pupils.
- Internet use, and the use of emerging technologies, such as iPads, is vital within today's workplaces. Children need to be taught how to use such technologies to equip them for the future.

Staff

All internet users within the school will be expected to sign an acceptable use agreement on an **annual basis** that sets out their rights and responsibilities and incorporates the school online safety rules regarding their internet use.
– see Appendix 1. Further details are given below.

Guidelines on ICT Use

Staff are welcome to use the Internet (including social networking sites), e-mail, mobile phones and other technologies during non-contact time (such as lunch time and after school.) However, the use of such technologies in lessons is forbidden. Disciplinary action will be taken against members of staff using the Internet, iPads, e-mail, mobile phones or any other information and communications technologies for non- teaching purposes in contact time.

Use the Internet and network responsibly. Close any Internet windows and log off from your account when you are not using a computer. If your account has been used by someone other than you without your knowledge, please alert the ICT co-ordinator or headteacher.

Supply teachers (and other temporary members of staff) are to use the following login details:
Username: Supply
Password: Password1
Any digital files which need to be left for a supply teacher should be left (clearly labelled with the class and date) in the 'Supply' folder in the StaffSharedArea folder.

Staff should use their school e-mail address (ending in @cchurchnw1.camden.sch.uk) for school purposes only. It should not be used to forward chain letters.

No member of staff should engage in direct communication (in or out of school) with a pupil who is not a member of their family by means of telephone, SMS text message, e-mail, Instant message (IM) or any other technology. Should special circumstances exist where such communication is felt to be necessary, the agreement of a line manager should be sought and professional language should always be used.

Further details of this can be found in the Social Media Policy.

Managing E-Mail

The Camden Education IT service creates accounts for staff and pupils (where appropriate, e.g. class accounts). Users will be given appropriate accounts and staff should change their password regularly.

The government now advises that whole class or project e-mail addresses are used within primary schools, rather than individual e-mail accounts.

There are some restrictions on staff e-mail addresses ending in @cchurchnw1.camden.sch.uk. These e-mail addresses should not be used to forward chain letters and should not be used for purposes not related to school. Please remember that when you use your

@cchurchnw1.camden.sch.uk e-mail address, it is similar to writing a letter on headed school paper; you are communicating on behalf of the school. Be professional.

Personal e-mail or messaging between staff and pupils should not take place.

Managing the Internet

The key to preventing children from accessing inappropriate material online is good planning and preparation. NEVER allow children to use a website that you have not seen before.

Learning to search the Internet for information is an important skill for children to learn. However, searches, particularly those for images, can be risky and present children with inappropriate material. If you are using a search engine such as www.google.co.uk, ensure that strict filtering is applied. Go the 'Preferences' to make such changes. The BBC search engine is a safer approach for children: http://search.bbc.co.uk/

Social networking sites, such as Facebook and Instagram, are not to be used by pupils in school.

The School Website

The school website (at www.cchurchnw1.camden.sch.uk) is hosted by LGFL and SLT are responsible for the content. The FTP address, username and password is held ONLY by SLT and senior ICT staff at Camden Local Authority. It is the responsibility of SLT to ensure that nobody else has access to the username and password.

The school website contains links to other educational sites. It is the responsibility of the ICT subject leader and SLT to ensure that such links are appropriate and do not contain material or adverts that may be offensive.

The school website contains photographs of pupils, at school and on educational visits. Children's names MUST NOT be used alongside photographs. Parents must give permission for their child's photograph to be used on the school website and a list of children whose images are not permitted to appear on the school website is kept by SLT.

Managing Personal Data

Pupil's personal details, including their full name, address, date of birth, telephone number, ethnicity, religion, previous schooling and SATs results are stored on the Administrators section of the network; only the school administration staff can access this area of the network and it is password protected. Integris software is used to store this data. The data is backed up on the server which means that it is also accessible by Camden Local Authority. The details of former pupils are also available.

This data is not accessible to other staff. It is stored in compliance with the Data Protection Act 1988.

Other school staff, including Senior Management and teachers, also store personal information about children, including class lists containing full names, date of birth and so on. This information is stored on the school network which can only be accessed by staff with a username and password.

Managing Emerging Technologies

Many emerging communications technologies offer the potential to develop new teaching and learning tools. However, it can be difficult to establish how safe a new technology is. Safety concerns may be around health, personal details or network security, for example.

At Christ Church, emerging technologies will be examined for educational benefit and a risk assessment will be carried out if it is thought their use would be beneficial in school.

School management should ensure that staff attend regular update training in order to ensure they can keep up with new developments in technology and any emerging safety issues.

Involving Parents

Children increasingly have access to the Internet, e-mail, iPads, mobile phones, Instant messaging (IM) at home. Unless parents are made aware of the possible dangers, pupils may be given unrestricted and unsupervised access. The school will lead online safety workshops for parents to make them aware of the dangers, recommend free filtering sites to limit what children can access and provide a list of websites with more information. Parents should also be informed that they can contact the school if they have any concerns about their child’s use of technology.

Responding to Incidents of Concern

Incidents of concern involving the use of information and communications technologies should be dealt with in the same manner as other child protection issues. In the first instance, talk to the designated child protection co-ordinator (currently Paula Walker) and fill in an incident of concern form (kept in the teacher's workroom.)

Incidents of concern involving illegal activity may require computers to be sealed and seized. In the case of an incident of concern involving information and communications technologies arising at school, please do not use the computer involved following the incident.

Incidents of concern involving information and communication technologies that arise outside of school will be treated as any other child protection matter would be, with the involvement of outside agencies, including the police, where necessary.

Responsibilities

Online safety is the responsibility of the ICT co-ordinator and the senior leadership team. All staff and adults within are the school are responsible for passing on incidents of concern to the designated child protection co-ordinator (currently Paula Walker).

Monitoring and Reviewing

The effectiveness of this policy will be continually considered by the ICT co-ordinator and senior leadership team in light of any incidents of concern. It will be reviewed regularly, taking new technologies into account.

Appendices

CHRIST CHURCH PRIMARY SCHOOL ACCEPTABLE USE STATEMENT (FOR STAFF)

The computer system is owned by the school and is made available to staff to enhance their professional activities, including teaching, research, administration and management. The school's ICT, online safety and Social Media Policies have 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.

All staff (including supply and temporary) requiring Internet access should sign a copy of this Acceptable Use Statement and return it to the SLT coordinator for approval.

1) I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the Headteacher or Governing Body.
2) I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
3) I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
4) I will not give out my own personal details, such as mobile phone number and personal email address, to pupils.
5) I will only use the approved, secure email system(s) for any school business.
6) I will ensure that personal data (such as data held on SIMS) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Headteacher or Governing Body.
7) I will not install any hardware of software without permission of the Headteacher.
8) I will only open email attachments from sources I know to be safe.
9) I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
10) Images of pupils and/ or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Headteacher.
11) I understand that all my use of the Internet and other related technologies can be monitored, logged and made available, on request, to the Headteacher.
12) I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the school community.
13) I will respect copyright and intellectual property rights.

14) I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.

15) I will support and promote the school's Online safety Policy and help pupils to be safe and responsible in their use of ICT and related technologies.

16) I will not access the school's wireless internet on personal mobile devices.

17) I will ensure that all personal devices (e.g. mobile phones, tablets, laptops) I bring into school are password protected.

18) Access to the internet and school server should only be made via the authorised account and password, which should not be made available to any other person.

19) It is the responsibility of staff members to make the ICT coordinator aware of occasions when passwords cease to become private.

20) Staff should ensure that high levels of data-protection are adhered to at all times. This means locking computers whilst leaving the room.

21) Issued netbooks/laptops are for staff use only.

22) Activity that threatens the integrity of the school ICT systems, or activity that attacks or corrupts other systems, is forbidden. Permission should be granted from the Headteacher before bringing in electrical and ICT equipment from home.

23) Users are responsible for all emails sent and for contacts made that may result in email being received.

24) Use for personal financial gain, gambling, political purposes, online shopping (other than that required for school-based purchases) or advertising is forbidden.

25) Posting anonymous messages and forwarding chain letters is forbidden.

26) As email can be forwarded or inadvertently be sent to the wrong person, the same professional levels of language and content should be applied as for letters or other media.

27) No reference should EVER be made to Christ Church Primary School on any social networking site.

28) Use of the network to access inappropriate materials such as pornographic, racist or offensive material is forbidden.

29) I understand this forms part of the terms and conditions set out in my contract of employment.

30) I agree to follow this code of conduct and to support the safe use of ICT throughout the school.

31) Any breaches in the operation of the requirements laid out in this Acceptable Use Statement will result in the Disciplinary Policy being invoked.

Full name: Signed: Date: