Christ THE Sower
Ecumenical Primary School (VA)

Online Safety and Acceptable Use Policy

May 2017

Vision for Learning

Our vision for learning at Christ the Sower states the type of learning community we aim to be, and places online learning – and consequently safety – in its proper context:

> **Believing that we can all excel, we are a community that deeply desires to learn. We nurture children and adults so that we are all empowered to be fearless, lifelong learners: embracing challenge, releasing creativity, persisting through difficulty, seeing mistakes as opportunity, discovering for ourselves and responding in wonder to what we find.**

Online safety is important in work that encompasses internet technologies and electronic communications such as mobile phones and wireless technology. It highlights the need to educate children and young people about the benefits and risks of using new technology and provides safeguards and awareness for users to enable them to control their online experiences. The general trend in mobile technologies is from the general to the personal, and thus whilst that brings about an immediacy of learning for children, it also brings threats much closer to their lives.

The school's online safety policy will operate in conjunction with other policies including those for Restorative Relationships, Curriculum, Data Protection and Child Protection and Safeguarding policies.

Good Habits of Learning and ICT Use

Online Safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff/pupils, encouraged by education and made explicit through published policies.
- Sound implementation of online safety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband from E2BN including the effective management of content filtering.
- National Education Network standards and specifications.

Online Safety Audit

This quick self-audit will help the senior leadership team (SLT) assess whether the online safety basics are in place.

The Policy was agreed by governors on:	*June 2017*
Date of latest update:	*May 2017*
The Policy is available for staff at:	*School website/safeguarding board in staffroom*
And for parents at:	*School website (about us/policies)*
The Designated Safeguarding Leads are:	*Huw Humphreys/Christine Richards/Kaajal Mushtaq/Sue Hodgetts*
Has the school an Online-Safety Policy that complies with MKSCB guidance?	Y/N
Has online safety training been provided for both pupils and staff?	Y/N
Is the Think U Know training being considered?	Y/N
Do all staff read and sign the Code of Conduct (with ICT use included) on appointment?	Y/N
Do parents sign and return an agreement that their child will comply with the School Online Safety Rules?	Y/N
Have school Online Safety Rules been set for pupils?	Y/N
Are these Rules displayed in all rooms with computers?	Y/N
Internet access is provided by an approved educational Internet service provider and complies with DfE requirements for safe and secure access.	Y/N
Has the school filtering policy has been approved by SLT?	Y/N
Is personal data collected, stored and used according to the principles of the Data Protection Act?	Y/N

The school has an online safety coordinator, Elspeth Whittle, and an online safety governor, Daniel Marshall. The online safety coordinator receives support from and reports to the team of Designated Safeguarding Leads. Our online safety Policy has been written by the school. It has been agreed by the senior management team and approved by governors. The online safety Policy will be reviewed annually. This policy will next be reviewed in March 2018.

Why is Internet Use Important?

The purpose of internet use in school is to broaden children's understanding of the world, to raise educational standards of achievement, to support the professional work of staff and to enhance the school's management information and administration systems. Internet use is part of the statutory curriculum and a necessary tool for learning. It is an essential element in 21st century life for education, business and communication. Access to the Internet is therefore an entitlement for pupils who show a responsible and mature approach to its use. Our school has a duty to provide pupils with safe, good quality Internet access. Pupils will use the internet and social media outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.

How does Internet Use Benefit Education?

Benefits of using the Internet in education include:

- access to world-wide educational resources including museums and art galleries;
- inclusion in the National Education Network which connects all UK schools;
- educational and cultural exchanges between pupils world-wide;
- access to experts in many fields for pupils and staff;
- professional development for staff through access to national developments, educational materials and effective curriculum practice;
- collaboration across support services and professional associations;
- improved access to technical support including remote management of networks and automatic system updates, exchange of curriculum and administration data with the Local Authority and DfE, and access to learning wherever and whenever convenient.

How can Internet Use Enhance Learning?

- The school internet access is designed expressly for pupil use; filtering is appropriate to the age of pupils.
- Pupils are taught what internet use is acceptable and what is not and given clear objectives for Internet use.
- Internet access is planned to enrich and extend learning activities.
- Staff should guide pupils in on-line activities that will support learning planned for the pupils' age and maturity.
- Pupils are educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- Pupils regularly learn about online safety across the computing curriculum, and in Y5/6 will participate in externally led workshops (www.jdsafeguarding.co.uk) or e-Cadets (https://www.ecadet.zone/) on how to make the safest use of modern technology.

Authorised Internet Access

- The school will maintain a current record of all staff and pupils who are granted Internet access.
- All staff must read and sign the 'Acceptable ICT Use Agreement' before using any school ICT resource.
- Parents will be informed that pupils will be provided with supervised Internet access.
- Parents will be asked to sign and return a consent form for pupil access.
- Pupils and parents will be required to read and sign an Acceptable Use Policy before using any ICT resources.

World Wide Web

- If staff or pupils discover unsuitable sites, the URL (address), time, content must be reported to the online safety coordinator or network manager.
- School will ensure that the use of Internet derived materials by pupils and staff complies with copyright law.
- Pupils should be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.

Email

- All pupils will have a Gmail account under the school's ctsmk.org.uk domain that can be used only to e-mail others within the school domain.
- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- Whole class or group e-mail addresses should be used in school
- The school, in cases where we believe that a safeguarding issue is likely, may block access in school to external personal e-mail accounts.
- E-mail sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.

Social Networking

- School will block/filter access to social networking sites and newsgroups unless a specific use is approved.
- Pupils are advised never to give out personal details of any kind which may identify them or their location
- Pupils should not place personal photos on any social network space.
- Pupils should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Pupils should be encouraged to invite known friends only and deny access to others.

Filtering

The school will work in partnership with the DfE and E2BN to ensure filtering systems are as effective as possible. Regular termly meetings between the DSL, online safety lead and the school's technical support for ICT, Theresa Stock, will examine the sites which the filtering has thrown up as being visited without authorisation.

Video Conferencing

Video conferencing is likely to become a more important technology in the future. At Christ the Sower, we use Skype on an internal system to contact classes. Any use of other video conferencing technologies must be planned and parents informed prior to class video conferences with other schools.

Managing Emerging Technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Staff should not use mobile phones to take pictures or videos of children. Staff should only use digital cameras which have been provided by the school. Mobile phones are not permitted for use anywhere in school, around the children, unless needed for a specific learning purpose by arrangement with the SLT (e.g. Plickers, or another app that records QR codes as responses to learning). This applies to members of staff and other visitors to the school. Mobile phones may only be used in office areas, staffroom etc. Teaching staff may take a mobile phone with them on a school trip/visit outside of school, for use in emergencies only.
- Children who bring mobile phones to school are required to hand them in to the school office staff or teacher every morning and devices are collected at home time.

The Prevent Duty and Online safety

- All schools have a duty to ensure that children are safe from terrorist and extremist material when accessing the internet in schools. We have an important role to play in equipping children to stay safe on line. Internet safety is integral to our computing curriculum. Our staff are aware of the risks posed by online activity of extremists and have a duty to take action if they believe the well being of any pupil is being compromised.

Published Content and the School Web Site

- The contact details on the Web site should be the school address, e-mail and telephone number. Staff or pupils personal information will not be published.
- The headteacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing Pupils' Images and Work on the School Website

- Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.
- Pupils' full names will not be used anywhere on the Website, and never in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Website.
- Work can only be published with the permission of the pupil and parents.

Information System Security

School ICT systems capacity and security will be reviewed regularly. Virus protection will be installed and updated regularly. Security strategies will be discussed with the Local Authority.

Protecting Personal Data and Assessing Risk

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer.
- Neither the school nor Milton Keynes Council can accept liability for the material accessed, or any consequences of Internet access.

Handling Online Safety Complaints

The school should audit ICT use to establish if the online safety policy is adequate and that the implementation of the online safety policy is appropriate. Complaints of Internet misuse will be dealt with by a senior member of staff.

- Any complaint about staff misuse must be referred to the Head teacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the complaints procedure.
- Discussions will be held with the Police Youth Crime Reduction Officer to establish procedures for handling potentially illegal issues.

Communicating this Policy

Pupils

- Rules for Internet access will be posted in all networked rooms.
- Pupils will be informed that Internet use will be monitored.

Staff

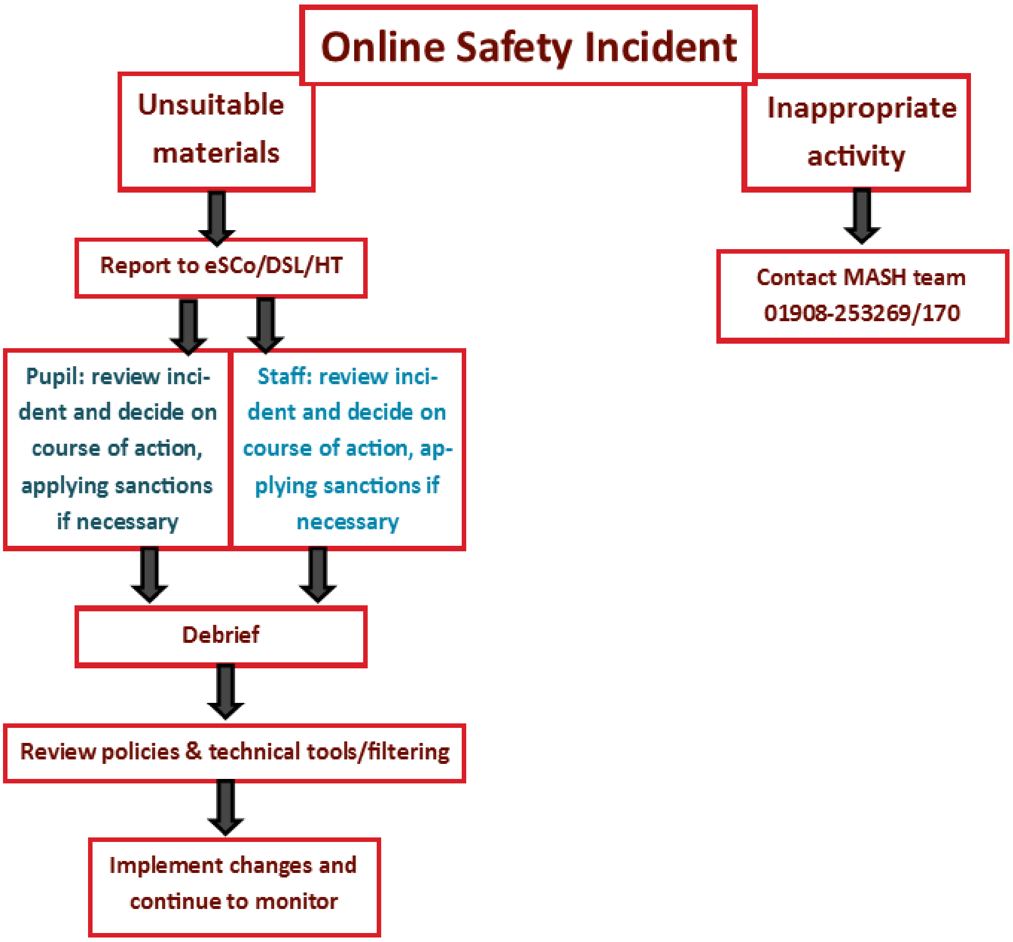
- All staff will be given the School Online safety Policy and its importance explained.
- All staff will be trained in Safeguarding procedures, including elements of Online safety and The Prevent Duty.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

Parents

- Parents' attention will be drawn to the School Online safety Policy in newsletters, the school brochure and on the school Web site. The school will also organise Online safety workshops to support parents' understanding of how to best safeguard their children against potential online dangers.

Updated November 2016
Referral Process – Appendix A
Online safety Rules– Appendix B
Letter to parents – Appendix C
Staff Acceptable Use Policy – Appendix D

Appendix A. Online Safety Flow Chart: referral process


Online Safety Incident
Unsuitable materials
Inappropriate activity
Report to eSCo/DSL/HT
Contact MASH team 01908-253269/170
Pupil: review incident and decide on course of action, applying sanctions if necessary
Staff: review incident and decide on course of action, applying sanctions if necessary
Debrief
Review policies & technical tools/filtering
Implement changes and continue to monitor

Appendix B. Online Safety Rules

Early Learning Phase Rules

THINK THEN CLICK: **These rules help us to stay safe on the Internet**

- We only use the internet when an adult is with us.
- We can click on the buttons or links when we know what they do.
- We can search the Internet with an adult.
- We always ask if we get lost on the Internet.
- We can send and open emails together.
- We can write polite and friendly emails to people that we know.

Middle and Upper Learning Phase Rules

These rules help us to stay safe on the Internet

- We ask permission before using the internet.
- We use websites that an adult has chosen, and those we choose ourselves when an adult is present.
- We tell an adult if we see anything we are uncomfortable with.
- We immediately close any webpage we are not sure about.
- We only email people within school.
- We send emails that are polite and friendly.
- We never give out personal information or passwords.
- We never arrange to meet anyone we don't know.
- We do not open e-mails sent by anyone we don't know.
- We do not use internet chat rooms.

Rules for Adults

These Online Safety Rules help to protect pupils and the school by describing acceptable and unacceptable computer use:

- The school owns the computer network and can set rules for its use.
- It is a criminal offence to use a computer or network for a purpose not permitted by the school.
- Irresponsible use may result in the loss of network or Internet access.
- Network access must be made via the user's authorised account and password, which must not be given to any other person.
- All network and Internet use must be appropriate to education.
- Copyright and intellectual property rights must be respected.
- Messages shall be written carefully and politely, particularly as email could be forwarded to unintended readers.
- Anonymous messages and chain letters are not permitted.
- Users must take care not to reveal personal information through email, personal publishing, blogs or messaging.
- The school ICT systems may not be used for private purposes, unless the head teacher has given specific permission.
- Use for personal financial gain, gambling, political activity, advertising or illegal purposes is not permitted.

Appendix C. Letter to Parents and Acceptable Use Agreement

Dear Mums, Dads and Carers

As part of our Information Communications and Technology scheme of work and general curriculum enhancement, Christ the Sower Primary school is providing supervised access to the Internet and e-mail. We are confident that this will benefit our children and equip them with important skills and knowledge in the wider world.

Our Internet Service Provider, E2BN, operates a filtering system that restricts access to inappropriate material, which is robust and which we check regularly. Children will always be supervised when using the Internet, and the rules of responsible Internet use will be explained to them at school.

The school will take all reasonable precautions to ensure online 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.

To support the policy, we ask you to sign the enclosed agreement. It would be helpful also if you would talk to your child about the 'rules' whenever necessary. Should you wish to discuss this agreement or any aspect of the Internet use, please contact me to arrange an appointment.

Yours sincerely
Huw Humphreys
Headteacher

Information and Communications Technology: Acceptable Use of Internet Agreement

Pupil and Parent Agreement

When I use the Internet and e-mail at school, I will keep to these rules:

- I will only use the Internet with permission, when there is a teacher or adult helper present.
- I will not try to find unsuitable sites on the Internet
- I will only e-mail people I know, or who my teacher has approved
- The messages I send will be polite and sensible
- I will not give my full name or home address or telephone number, or arrange to meet someone unless my parent, carer, or teacher has given permission.

Pupil's signature ………………………………………………………………………….. **Date:** ……………………

Parent

As the parent or legal guardian of the pupil signing above, I give permission for my son or daughter to use electronic mail and the Internet, under supervision at school. I understand and accept the above rules for acceptable use of the Internet and will discuss these with my child.

Parents' signature ………………………………………………………………………… **Date**………………………

Pupil's name …………………………………………………

Class ……………………………………………………………

Appendix D: Staff Information Systems Code of Conduct (explanation of paras 4.23 and 4.24 of Code of Conduct)

To ensure that staff are fully aware of their professional responsibilities when using information systems, they are asked to sign this code of conduct. Staff should consult the school's online safety policy for further information and clarification.

- The information systems are school property and I understand that it is a criminal offence to use a computer for a purpose not permitted by its owner.
- I will ensure that my information systems use will always be compatible with my professional role.
- I understand that school information systems may not be used for private purposes, without specific permission from the headteacher.
- I understand that the school may monitor my information systems and Internet use to ensure policy compliance.
- I will respect system security and I will not disclose any password or security information to anyone other than an appropriate system manager.
- I will not install any software or hardware without permission.
- I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will respect copyright and intellectual property rights.
- I will report any incidents of concern regarding children's safety to the school Online safety Coordinator or the Designated Child Protection Coordinator.
- I will ensure that any electronic communications with pupils are compatible with my professional rôle.
- I will promote Online safety with pupils in my care and will help them to develop a responsible attitude to system use and to the content they access or create.

The school may exercise its right to monitor the use of the school's information systems, including Internet access, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

I have read, understood and agree with the Information Systems Code of Conduct.

Signed: ……………………………… Capitals: ……………………… Date: …………….

Accepted for school: ……………………………. Capitals: …………………………