Christ Church C.E.(VC) Primary School E-Safety Policy

Introduction

This policy is written in conjunction with North Yorkshire e-safety guidance and the safeguarding audit.
Pupils, parents and staff are included in the development of this school e-Safety policy as well as the Governing Body.
This policy reflects Christ Church C.E.(VC) School's decisions on balancing educational benefit with potential risks. It is used in conjunction with policies relating to curriculum, data protection, anti-bullying, safeguarding children, security and home-school agreements.

Mrs S. Bennett the headteacher is identified as the e-safety co-ordinator.
This policy has been prepared by the e-safety co-ordinator and has been agreed by the Headteacher and Governing Body.

Date published: 01/02/2016
Date of next review (at least annually): 01/02/2017

Rationale

The internet and other digital technologies permeate all aspects of life in a modern technological society. Internet use is part of the statutory National Curriculum and is a necessary tool for staff and pupils. It is the entitlement of every pupil to have access to the internet and digital technologies, in order to enrich his/her learning.

Scope

This policy applies to all pupils, all teaching staff, all support staff, all governors and all volunteers.

Aims

Our aims are to ensure that all pupils, including those with special educational needs:

- will use the internet and other digital technologies to support, extend and enhance their learning;
- will develop an understanding of the uses, importance and limitations of the internet and other digital technologies in the modern world including the need to avoid undesirable material;
- will develop a positive attitude to the internet and develop their ICT capability through both independent and collaborative working;
- will use existing, as well as up and coming, technologies safely.

Internet use will support, extend and enhance learning

- Pupils will be given clear objectives for internet use.
- Web content will be subject to age-appropriate filters.
- Internet use will be embedded in the curriculum.

Pupils will develop an understanding of the uses, importance and limitations of the internet

- Pupils will be taught how to effectively use the internet for research purposes.
- Pupils will be taught to evaluate information on the internet.
- Pupils will be taught how to report inappropriate web content.
- Pupils will develop a positive attitude to the internet and develop their ICT capability through both independent and collaborative working.
- Pupils will use the internet to enhance their learning experience.
- Pupils have opportunities to engage in independent and collaborative learning using the internet and other digital technologies.

Pupils will use existing technologies safely

- Pupils will be taught about e-safety
-

Data Protection

- There is a separate Data Protection policy.

E-mail

- Pupils and staff will only use approved e-mail accounts when using the school network.
- Pupils will tell a member of staff if they receive inappropriate e-mail communications.
- Pupils will only use e-mail (VLE Logins)for approved activities.

Internet Access and Learning Platform

- Staff will read and sign the *NYCC Acceptable Use Policy – ICT and e-Technology* before using any school ICT resource. See Appendix A.
- Parents will read through the Acceptable Use Agreement (Appendix B) with their child before it is signed. This will be done before their children are given access to internet resources (including the Learning Platform).
- Pupils will be taught to use the internet responsibly and to report any inappropriate content to a responsible adult.
- Pupils will be taught the purpose of filtering possible misuse of words and the purpose of the 'whistle' on all pages of the VLE. This reports possible inappropriate use to the HT, AHT and ICT lead.

Mobile Phones and other handheld technology

We recognise that mobile phones are part of everyday life for many children however children are not permitted to bring mobile phones on educational visits of stays or to school, except where permission has been given for walking alone. If permission has been given, phones must be handed in at the office and collected at the end of the day. This is in conjunction with the school's mobile phone policy.

When pupils are using mobile technology (their own or that provided by the school) they will be required to follow the school's Acceptable Use Policy (AUP).

Such items can be confiscated by school staff if they have reason to think that they are being used to compromise the wellbeing and safety of others (*Education and Inspections Act 2006, Sections 90, 91 and 94)*

Systems Security

- ICT systems security will be regularly reviewed with support from Schools ICT.

Web Filtering

- The school will work with Schools ICT to ensure that appropriate filtering is in place.
- Pupils will report any inappropriate content accessed to an appropriate member of staff.

Communication of the e-safety policy to pupils

- Pupils will read (or be read) and sign the age-appropriate Internet and Learning Platform Acceptable Use Policy before using these resources. These are printed in their home/school link books. See Appendix B.
- E-safety rules will be posted in each room where a computer is used.
- Pupils will be informed that internet and Learning Platform use will be monitored.
- e-Safety will be included in the curriculum and regularly revisited.

Communication of the e-safety policy to staff

- The e-safety and acceptable use policies will be given to all new members of staff as part of the staff handbook.
- The e-safety and acceptable use policies will be signed by all staff and discussed with them at least annually.
- Staff will be informed that internet and Learning Platform use will be monitored.

Communication of the e-safety policy to parents/carers

- The acceptable use policies will be available in the school prospectus and on the school website.
- The school website and Learning Platform (where applicable) will include a list of e-safety resources and information for parents to access.
- Parents are given information via the home school link books when their child joins the school. This will include acceptable use policies relating to the internet, Learning Platform and other digital technologies.
- The school will communicate and publicise e-safety issues to parents through the school newsletter, website and Learning Platform.

e-safety Complaints

- Instances of pupil internet or Learning Platform misuse should be reported to a member of staff.
- Staff will be trained so they are able to deal with e-Safety incidents. They must log incidents reported to them and if necessary refer the matter to a senior member of staff.

- Instances of staff internet or Learning Platform misuse should be reported to, and will be dealt with by, the Headteacher.
- Pupils and parents will be informed of the consequences of internet and/or Learning Platform misuse.

Whole-School Responsibilities for Internet Safety

Headteacher

- Responsible for e-safety issues within the school but may delegate the day-to-day responsibility to a Senior Leader as the e-safety co-ordinator.
- Ensure that the e-safety co-ordinator is given appropriate time, support and authority to carry out their duties effectively.
- Ensure that developments at Local Authority level are communicated to the e-safety co-ordinator.
- Ensure that the Governing Body is informed of e-safety issues and policies.
- Ensure that appropriate funding is allocated to support e-safety activities throughout the school.

e-Safety co-ordinator (ideally as part of a wider child protection role)

- Primary responsibility: establish and maintain a safe ICT learning environment (under the direction of Senior Management).
- Establish and maintain a school-wide e-safety programme.
- Form a school e-safety team to review and advise on e-safety policies.
- Work with the e-safety team to develop, and review, e-safety policies and procedures.
- Respond to e-safety policy breaches in an appropriate and consistent manner in line with protocols set out in policies, and maintain an incident log.
- Form a school e-safety management team to review the effectiveness and impact of the policy.
- Establish and maintain a staff professional development programme relating to e-Safety.
- Develop a parental awareness programme.
- Develop an understanding of relevant legislation and take responsibility for their professional development in this area.

Governing Body

- Appoint an e-Safety Governor who will ensure that e-safety is included as part of the regular review of child protection and health and safety policies.
- Support the Headteacher and/or designated e-safety co-ordinator in establishing and implementing policies, systems and procedures for ensuring a safe ICT learning environment.
- Ensure that appropriate funding is authorised for e-safety solutions, training and other activities as recommended by the Headteacher and/or designated e-safety co-ordinator (as part of the wider remit of the Governing Body with regards to school budgets).
- Promote e-safety to parents and provide updates on e-safety policies within the statutory ‘security’ section of the annual report.

Network Manager/Technical Support Staff

- Provide a technical infrastructure to support e-safety practices.
- Ensure that appropriate processes and procedures are in place for responding to the discovery of illegal materials, or suspicion that such materials are, on the school's network.
- Ensure that appropriate processes and procedures are in place for responding to the discovery of inappropriate but legal materials on the school's network.
- Develop an understanding of relevant legislation.
- Report network breaches of acceptable use of ICT facilities to the Headteacher and/or the e-safety co-ordinator.
- Maintain a professional level of conduct in their personal use of technology, both within and outside school.
- Take responsibility for their professional development in this area.

Teaching and Support Staff

- Contribute to the development of e-safety policies.
- Adhere to acceptable use policies.
- Take responsibility for the security of data.
- Develop an awareness of e-safety issues, and how they relate to pupils in their care.
- Model good practice in using new and emerging technologies.
- Include e-safety regularly in the curriculum.
- Deal with e-Safety issues they become aware of and know when and how to escalate incidents.
- Maintain a professional level of conduct in their personal use of technology, both within and outside school.
- Take responsibility for their professional development in this area.

Wider School Community

- This group includes: non-teaching staff; volunteers; student teachers; other adults using school internet, Learning Platform or other technologies.
- Contribute to the development of e-safety policies.
- Adhere to acceptable use policies.
- Take responsibility for the security of data.
- Develop an awareness of e-safety issues, and how they relate to pupils in their care.
- Model good practice in using new and emerging technologies.
- Know when and how to escalate e-safety issues.
- Maintain a professional level of conduct in their personal use of technology, both within and outside school.
- Take responsibility for their professional development in this area.

Parents and Carers

- Contribute to the development of e-safety policies.
- Read acceptable use policies and encourage their children to adhere to them.

- Adhere to acceptable use policies when using the school internet and/or Learning Platform.
- Discuss e-safety issues with their children, support the school in its e-safety approaches and reinforce appropriate behaviours at home.
- Take responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.
- Model appropriate uses of new and emerging technologies.
- Liase with the school if they suspect, or have identified, that their child is conducting risky behaviour online.

Appendix A

Christ Church C.E (VC) Primary School
Acceptable Use Agreement – ICT and E Technology

This agreement is designed to ensure that all members of staff are aware of their professional responsibilities when using any form of technology. Technology relates to ICT systems, hardware, software, internet, email, Learning Platforms, web2 technologies, mobile devices, cameras, laptops and memory devices.

Members of staff:

- Must only use the school's technologies for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body. It is a criminal offence to use an ICT system for uses other than those permitted by its owner.
- Must only use approved email systems for any school business.
- Must not browse, download or send material that could be considered offensive, and should report any accidental access of inappropriate materials to their line manager.
- Have a duty to protect their passwords and personal network and Learning Platform logins, and should log off the network and Learning Platform when leaving a workstation unattended. Any attempts to access, corrupt or destroy other users' data, or compromise the privacy of others in any way, using any technology, is unacceptable.
- Must not install any software or hardware without permission from a technician or the ICT coordinator.
- Are not permitted to use personal portable media for storage of school related data/images (e.g. USB stick) without the express permission of the Headteacher. If in doubt, check.
- Should ensure that personal data (such as data held on the admin system) is kept secure and is used appropriately, whether in school, taken off school premises, or accessed remotely. Personal data can only be taken out of school when authorised by the Headteacher or Governing Body.
- Are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, including when on external trips/visits. With the written consent of parents (on behalf of parents) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment. Digital images are easy to capture, reproduce and publish and, therefore, misused and so their use is monitored closely.
- Should ensure that their use of web 2 technologies, including social networking sites, such as Facebook, Bebo, and Myspace, does not question or bring their professional role into disrepute. Members of staff:
  - Are advised to consider, and set appropriately, their privacy settings on such sites.
  - Should consider the appropriateness of images and material posted. Once posted online, a message, photo or video clip can be freely copied, manipulated and circulated and will potentially exist forever.
  - Should not communicate with pupils, in relation to either school or non school business, via web 2 technologies. Members of staff should only communicate with pupils using the appropriate LA/school learning platforms or other systems approved by the Headteacher.
- Are not permitted to contact or communicate with pupils, parents or conduct school business using personal email addresses or telephones, without specific permission from the Headteacher.
- Should not give out their own personal details, such as telephone/mobile number or email address, to pupils.
- Must ensure that all electronic communication with pupils and staff is compatible with their professional role.
- Must promote and model positive use of current and new technologies and e-safety. Members of staff can access information about e-safety from the North Yorkshire Primary ICT room and within the North Yorkshire Learning Platform and from the Learning Network. The e-safety coordinator can also provide information, resources and guidance.
- Must respect and comply with copyright and intellectual property rights.
- Have a responsibility to report any misuses of technology, including the unacceptable conduct of others, to the e-safety coordinator or Headteacher.

User Signature

I agree to follow this user agreement, and understand that failure to do so may result in disciplinary proceedings in the line with the School's Disciplinary Procedure.

Signature ..... Date .....

Full Name (Printed) ..... Job Title .....

Appendix B

Christ Church C.E(VC) Primary School

ICT Acceptable Use Policy

When using the school's ICT equipment and other information systems, I have understood and will follow these guidelines:

- I have read and know what the computer rules in this document mean to me.
- I will only log on to the computers, PurpleMash, DB Primary and SumDog using my own username and password.
- I will not share my password.
- If I think someone has logged in as me I will tell a teacher.
- I will not look for, save or send anything that could be unpleasant or hurtful.
- I will make sure I take care of any ICT equipment.
- I will not install any software on school computers.
- I know that my use of ICT is checked and that parents/carers contacted if there is concern.
- I will not eat or drink while using ICT equipment.

Social Media

- I know that some websites and social networks have age restrictions and I should not use them unless I am old enough.
- I will not comment about any pupil or member of staff online.
- I will not give away any personal details.
- I will not use any photographs without permission.
- If I see anything that concerns me, I will report it to an adult.

Managing Digital Content/Email

- I will not publish anything online, e.g. images or pictures, without asking my teacher.
- I will take care in opening any attachments sent by email. I will not open an attachment, or download a file, unless I know and trust the person who has sent it.
- When sending emails I will make sure that they are appropriate.

Mobile phones and devices

- I will only bring my mobile phone or other devices to school with permission from my teacher and written permission from home.
- I understand that the school accepts no liability for the loss or damage of these devices.
- I will not take pictures in school on my mobile phone or mobile device.

Agreement

I agree to follow the rules set out in this AUP.
I know that if I break any of these rules my parent/carer will be told.

Name: _____ Signature: _____