North Cerney C of E Primary Academy

Our School Vision
To enthuse, encourage and enable our pupils to seek challenges, explore beyond boundaries, communicate confidently and cooperatively, show initiative, self-discipline, respect and open mindedness, all within the framework of Christian Values.

Acceptable Use Policy for the Internet

Giving our pupils *faith* in their future

The draft policy was ratified and approved by Governors on:

Date of Policy: **March 2013**

Reviewed annually

Senior staff responsible: Headteacher

This policy was formulated by a working party consisting of the Headteacher, Governors and a teacher.

North Cerney C of E Primary School

Acceptable Use Policy for the Internet

The school policy for Acceptable Use of the Internet reflects the consensus of opinion of the whole teaching staff and has the full agreement of the Governing Body.

Introduction

"Children and young people have embraced new technologies as a source of information, education and entertainment. The use of digital technology has been completely normalised and it is now fully integrated into their daily lives. Children are using technology in new and exciting ways, enhancing and enriching their lives with the many tools on offer".
"ICT can offer many positive educational and social benefits to young people but unfortunately there are some dangers. As in any other area of life, children and young people are vulnerable and may expose themselves to danger, whether knowingly or unknowingly, when using the internet and other technologies".

Signposts to e-safety
Becta 2007

Aims

Access to life-long learning and employment increasingly requires the use of a range of information technologies and pupils need to develop life skills for their use. The internet, as an open, public communications channel is just one aspect of this. This policy relates to the school's Internet environment and is part of a suite of e-safety documents and strategies developed to ensure pupils are provided with as safe and secure Internet environment as is possible, and are educated to be aware of, and respond responsibly, to any risks.

The policy identifies the measures in place in our school

- to protect children from undesirable content on the Internet
- to protect them from undesirable contacts over the Internet,
- to prevent unacceptable use of the Internet by children or adults
- to address issues of copyright for materials published on the Internet

Roles and responsibilities

E-safety is a whole-school responsibility dependent on all stakeholders e.g. staff, governors, advisers, parents and, where appropriate, pupils themselves taking responsibility for the use of the Internet and other forms of communication. Of major importance in creating a safe e-learning environment is the internet safety education which occurs in the classroom itself, initiated by the teacher or teaching assistant. Whilst the Headteacher has overall responsibility for e-safety issues, the ICT Coordinator has delegated responsibility as the E-safety Coordinator responsible for e-safety management.

E-learning technologies

Internet access is supplied by KCOM which provides an effective and safe e-learning environment including Internet access and e-mail service. To safeguard against risks and unacceptable materials and activities these services include filtering and content control, firewall and virus protection, and monitoring systems. All new Internet technologies will only be made accessible to the school e-community when they have been assessed for their nature, content, educational benefit, safety and security.

Permission to use the Internet

The Internet can provide pupils and all stakeholders with opportunities to experience and use a wide range of activities, resources, and information to support and enhance the learning and teaching across the whole school curriculum. All pupils will be expected to access the Internet unless parents have indicated otherwise at the time their child is admitted to school.
Parents will be asked to discuss with their children the e-safety agreement and sign the agreement. Without this being signed pupils will not be allowed to access the Internet.

Accessing and using the Internet

In lessons the majority of access to the Internet will be by the teacher, by adult demonstration or through carefully supervised access to specific approved on-line materials. Pupils will be taught how to use the internet safely and responsibly as an integral part of e-learning across the curriculum. Pupils will be taught how to be safe while online at home as well as at school.

Google and Yahoo (standard version) are not to be used by pupils. If staff wish pupils to access sites or materials listed by one of these search engines they will need to separately create / save to a folder of suitable images or compile a list of hyperlinks to suitable web addresses in an offline document which children can then use to link straight to verified and tested websites. Keyword search skills can be taught using the learning technologies to which the school subscribes and through software simulating search engines (Young Explorer)

E-safety – Content

Unintentional exposure of children to Inappropriate Content

It is the School's policy that every reasonable step should be taken to prevent exposure of children to undesirable materials on the Internet. It is recognised that this can happen not only through deliberate searching for such materials, but also unintentionally when a justifiable Internet search yields unexpected results.
To protect children from such occurrences, the school has adopted the following position:

In-school protection by:

- adult supervision of pupils' Internet activity, with no accessing or searching of the Internet allowed without a suitable adult present in the room
- the 'caching' of Internet sites whenever possible in advance by staff to verify the site and its content
- children will be taught to become critical and discriminating users of materials they find online, through questioning the source and reliability of any content they access and by being aware of ways to minimise risks

- if any users discover undesirable sites, the URL (address) and content must be reported to the ICT Coordinator who will inform the Headteacher as soon as possible
- the use of the accredited Broadband Service which provides protection by maintaining a list of approved sites
- filtering, such as blocking strategies, allowed lists, dynamic filtering, rating systems, flagging systems and monitoring
- the imposition of a 'banned list' of undesirable sites
- the filtering of sites by language content with prohibition of sites with unacceptable vocabulary
- 'live' anti-virus protection

Intentional access of undesirable content by children

Children should never intentionally seek offensive material on the Internet. In such instances these steps will be followed. Any such incident will be treated as a disciplinary matter, and the parents of a child or children will be informed.
In the event of children being exposed to undesirable materials, the following steps will be taken:

- Pupils will notify a teacher or teaching assistant immediately
- Initially the e-safety coordinator will be notified by the teacher, and then the Headteacher (as child protection officer)
- The incident will be recorded in a central log, located in the school office, by which the school may reliably report the frequency and nature of incidents to any appropriate party
- The County approved forensic monitoring software will be used to investigate as appropriate
- Parents will be notified at the discretion of the Headteacher according to the degree of seriousness of the incident (for example, exposure to materials that include common profanities might not be notified to parents, but exposure to materials that included pornographic images would be notified)
- The Headteacher will regularly notify Governors of any incidents involving inappropriate or unacceptable use of school internet / ICT facilities as part of the Headteacher's safeguarding report.

Intentional access to undesirable content by adults

Deliberate access to undesirable materials by adults is unacceptable, and will be treated as a disciplinary issue. If abuse is found to be repeated, flagrant or habitual, the matter will be treated as a very serious disciplinary issue. The Governors will be advised and the DGAT will be consulted.

Risks associated with Contact

The Internet as a means to contact people and organisations is an extremely valuable tool, encouraging the development of communications skills and transforming the learning process by opening up extra possibilities. However, just as in the real world, children may get involved in inappropriate, antisocial or illegal behaviour while using new technologies e.g. cyber bullying, identity theft, and arranging to meet people they have met online.

Whilst children will, at times, use emails as part of their learning across the curriculum, the school does not use chat rooms or instant messaging. Children will however be made aware of the risks involved in all of these and ways of avoiding them, as part of their e-safety and digital literacy skills development.

Receiving and sending of e-mails by children

It is recognised that e-mail messages received by children can contain language or content that is unacceptable and that some people may try to use e-mail to identify and contact children for unacceptable reasons. If any member of staff believes that a child has been targeted with e-mail messages by parties with criminal intent, the messages will be retained, the incident recorded, and the Governors and the child's parents informed. Advice will also be taken regarding possible further stops, including investigation using forensic monitoring software.

To avoid these problems the school has adopted the following practice:

- The use of the accredited County e-mail service which includes filtering all incoming and outgoing messages for inappropriate content and spam
- Pupils read e-mail messages when a member of staff is present, or the messages have been previewed by the teacher
- Children are taught not to open or respond to emails from a previously unknown source, but to tell the member of staff present in the room so that appropriate action can be taken
- Steps are taken to verify the identity of any school or child seeking to establish regular e-mail with this school
- Pupils save their emails / messages to Draft for the teacher or teaching assistant to approve before being sent (as they would with a conventional letter)
- To avoid children revealing their identity within e-mail messages, only the child's forename is revealed: when appropriate 'internet aliases' are used for each child: the child's personal address is never revealed, and information is never given that might reveal the child's whereabouts.

Other use of the Internet and email facilities

The school internet / e-mail facilities should only be used for educational purposes during teaching and learning time. Staff are advised not to, but if they do choose to use school internet facilities for personal purposes, such as online banking or purchasing of items for personal use, this will be at their own risk.
Inappropriate use will be subject to similar procedures as those listed above.
Staff should be mindful of unsolicited emails from people they do not know and use the Spam reporting facility as appropriate.

Publishing of Content on the Internet

It is recognised that staff and children may at some time produce and publish materials on an Internet Website associated with the School or the County.
The school has its own website hosted through its recognised reputable ISP. Materials produced as part of children's learning may be published on it unless parents have indicated otherwise at the time their child is admitted to school.
No materials will be published on the Internet which contains any unacceptable images, language or content. Infringement of this rule will be taken as a serious disciplinary issue.

Use of the school's Internet facility by visitors and guests

Members of school staff are expected to take responsibility for the actions of any adult guests or visitors who they allow or encourage to use the school Internet facilities. The essential 'dos and don'ts' are explained to such visitors and guests prior to their use of the Internet.
Unacceptable use will lead to the immediate withdrawal of permission to use the school Internet facility.

Copyright Issues

It is recognised that all materials on the Internet are copyright, unless copyright is specifically waived. It is the school's policy that the copyright of Internet materials will be respected.

Where materials are published on the Internet as part of the teacher's professional duties, copyright will remain with the County Council. Internet published materials will contain due copyright acknowledgements for any third party materials contained within them.

Related documents and guidance

School e-safety awareness materials

- Pupil / parent user agreement and information leaflets
- E-safety education programme (for all year groups – Hectors World)
- E-safety posters

The E-Safety Policy: Rights & Responsibilities

Pupil Rights

Pupils will be reminded each term of how to protect themselves whilst using the internet and mobile phones.

Pupils will be reminded each term how to report accidental access to inappropriate materials.

Pupils will be reminded each term about the sanctions for deliberate access to inappropriate materials.

Pupils will be involved in the review of internet safety via the school council.

Parent Rights

Parents will be able to view a copy of the Pupil AUP on the school web site.

Parents will be informed and invited to be involved in the review of e-safety policies.

Parents will be advised on ICT use at home and given contact details of organisations involved in E-Safety.

Parents can restrict the use of images of their children by filling in a form found in the office and on the web site.

Staff Rights

Staff will be offered training to safeguard themselves.

Staff will be offered training to deliver the e-safety programme.

Staff will be given lesson plans and resources to deliver the e-safety programme.

Head: Responsibilities

Take ultimate responsibility for internet safety issues.

Ensure all data is used in accordance with the Data Protection Act.

Offer additional advice and supervision to pupils with learning difficulties or disabilities.

Inform KCOM if pupils or staff access inappropriate information through the internet accidentally.

Inform KCOM, The DGAT or the Police if anyone deliberately accesses inappropriate information through the internet.

Enforce appropriate sanctions should be for deliberate or careless breaches of this policy.

Ensure that developments at local and partnership level are communicated to the internet safety team

Ensure that the governing body is informed of the issues and the policies

Delegate day-to-day responsibility to the teaching staff

Ensure that the internet safety team has the authority and time to carry out the duties effectively

Ensure that appropriate funding supports the technical infrastructure and Inset training.

Support the internet safety team in creating an internet safety culture within the school.

Ensure staff are aware of the sanctions for breaches of the AUP

Governors: Responsibilities

Appoint a governor with specific responsibility for ICT.

Be aware of the risks of using ICT in schools

Include Internet safety in the regular review of child protection and health and safety policies

Devise a strategy for dealing with the media should serious incidents occur.

Secure funding for internet safety solutions and training.

Update Internet safety policies within the statutory 'security' section of the annual report.

Agree a set of appropriate sanctions for possible breaches of the staff AUP.

Develop an understanding of existing school policies, systems and procedures for maintaining a safe ICT learning environment

Promote Internet safety information to parents

ICT Safety Coordinator/Team: Responsibilities

Review this policy yearly with the Head to assess its effectiveness.

Publish links and information about E-Safety for staff, pupils and parents on the web site.

Advise parents to monitor their child's use of the Internet at home.

Ensure all web site pages are reviewed by a trained member of staff before being published.

Ensure pupils' full names are not be used for image labels, file names or tags.

Establish and maintain a school-wide internet safety programme.

Provide given lesson plans and resources for staff to deliver the e-safety programme to pupils.

Offer training for staff to understand issues and their responsibilities for pupils' safety.

Ensure new staff and pupils are made aware of Internet safety policies

Assess pupils' understanding of safety issues at the end of the year.

Use all data according to the data protection act.

Provide anti-virus protection, filtering and monitoring software on all machines.

Work towards a school-wide network with individual logins for all staff for all machines.

Ensure all workstations log off automatically.

Maintain a log of all incidents, preserve evidence and inform the head teacher, about policy breaches.

Update the Head, staff and governors on current internet safety issues.

Liaise with outside agencies.

Ensure that appropriate and effective electronic security systems are in place, such as filtering, monitoring and firewall technology, and virus protection.

Monitor computer networks regularly.

Ensure that staff computers are secure.

Staff: Responsibilities

All staff must sign the Staff AUP and follow it when using school equipment.

Any breaches of the AUP must be reported to the head teacher.

The AUP and Teacher Responsibilities must be kept with your notebook/laptop.

Be professional in your own internet use within and outside school

All pupils will receive one e-safety lesson in each of the six terms.

Remind pupils of the risks and responsibilities whenever ICT is used and post pupil AUP in class

Any disclosure by a pupil involving computers at home should be passed to the head.

Evaluate all web sites in advance of classroom use.

Position computers so pupils can be supervised and plan use of ICT so that safety is not compromised

Differentiate access to online resources for pupils with different abilities.

Embed internet safety messages within the curriculum.

Develop and maintain knowledge of internet safety issues via CPD

Images of pupils should be only stored on the server in the RM Staff folder.

Staff should not store data or images of pupils on class computers or **personal** digital equipment such as mobile phones.

Any stored data and images must be deleted when no longer required.

All staff Email addresses must be protected by a secure password.

All classroom computers and laptops must be switched on daily and connected to the internet to update the virus software.

Any technical problems should be reported on the Staff Portal ICT log.

All staff must log out of computers and email accounts when not using them.

Mobile storage devices (memory sticks etc) must be virus checked before opening any files if they are used on computers not belonging to the school. Any problems must be reported and the device must no longer be used.

Staff should store all their work related data on memory sticks and back these up on their laptop weekly.

Staff ICT Acceptable Use Policy

Please read this policy carefully as you will be deemed to be aware of its contents.

- **Use of computers must always be lawful and appropriate.**
- **Use of computers must not involve risks to the integrity of information and computer systems.**
- **Use of computers must not damage the school's or any individual's reputation.**
- **All users should use the Internet responsibly and should not be involved in any activity that that relates to:**
  - pornography
  - promoting discrimination
  - promoting racial hatred
  - promoting religious hatred
  - promoting illegal acts
  - any other offensive act
- Staff must not use facilities for running a private business
- Staff must not reveal confidential information, which includes financial information, personal information, information contained in databases, access codes, and business relationships
- Staff must not intentionally interfere with the internet connection, including actions which might allow computer viruses access or sending/receiving of large amounts of data.
- Staff must not upload, download, or otherwise transmit copyrighted materials such as music and video files.

Monitoring

KCOM monitor and audit Internet use to see if users are complying with the policy. Any potential misuse identified by KCOM will be reported to the school.

N.B. Necessary access to any site deemed 'inappropriate' for educational use should be recorded in your planning.

Incidents which appear to involve deliberate access to web sites, newsgroups and online groups that contain the following material will be reported to the police:

- sexual images of children, apparently under 16 years old.
- material that breaches the Obscene Publications Act in the UK
- criminally racist material.

If inappropriate material is accessed **accidentally**, users should immediately report this to the SWGfL:

support@swgfl.org.uk 0870 9081 708

I have read and understood this policy and agree to abide by the conditions when working for and/or using any equipment provided by North Cerney C of E Primary School.

Name: _____ Signed: _____ Date: _____

North Cerney Church of England Academy Trust

E-Safety agreement

(This agreement was put together by a working party of pupils and teachers)

For my own personal safety – at home!

- I will ask permission from a member of staff before using the Internet at school.
- I am aware of "stranger danger" when on line and will not agree to meet online friends.
- I will tell an adult about anything online which makes me feel uncomfortable.
- When in school I will only contact people with my teacher's permission.

To keep the system safe – at school!

- I will ask permission from a member of staff before using the Internet at school.
- I will not try to bypass the system to reach websites the school has blocked.
- I will not access other people's files without permission.
- I will not play games on a school computer unless my teacher has given me permission.
- I will not install software on school computers.
- I will not use the system for shopping, or uploading videos or music.
- I will not put my "Personal Information" online. (My full name, birthday, phone number, address, postcode, school etc.)

Responsibility to others

- The messages I send will be polite and responsible.
- I will not upload images or videos of other people without their permission.
- Where work is copyrighted (including music, videos and images,) I will not either download or share with others.
- I understand that the school may take action against me if I am involved in inappropriate behaviour on the internet and mobile devices.
- I will not bring in mobile phones or cameras in to school. Other devices (e.g. games consoles, cameras) should not be brought into school, unless my teacher has given me permission.

Pupils E-safety contract

Please complete, sign and return to the class teacher.	
Pupil:	Class:
Pupil's Agreement: I have read and I understand the pupils e-safety agreement, and will abide by the rules which are designed to keep both myself and the school safe	
Signed:	Date:
Parent's Consent: I have read and understood the e-safety agreement and give permission for my son / daughter to access the Internet at school, and will encourage them to abide by these rules. Children will receive advice on e-safety at school, advice for parents is available at www.thinkuknow.org.uk/parents or on the school website. I understand that the school will take reasonable precautions to ensure pupils cannot access inappropriate materials. I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's e-safety. I will ensure that any pictures taken during school events that include other children will not be shared using social media.	