Newland St. John's C.E. Primary School

eSafety Policy

To be read in conjunction with the Information and Communications Technology (ICT) policy, the End-user Acceptable Use Policies (AUPs) and the Child Protection Policy.

Introduction

The school recognises that the Internet and other digital technologies have an important role in the learning and teaching process and aims to provide opportunities for enhancing children's learning through access to these technologies. It is important to balance the benefits with an awareness of the potential risks and our eSafety policy reflects the school's commitment to the safeguarding and well-being of our pupils as set out in the Every Child Matters agenda.

The policy has been drawn up in accordance with the guidelines set out by the Yorkshire and Humberside Grid for Learning (YHGfL).

Responsibilities of the School Community

We believe that eSafety is the responsibility of the whole school community, and that everyone has their part to play in ensuring all members of the community are able to benefit from the opportunities that technology provides for learning and teaching. The following responsibilities demonstrate how each member of the community will contribute.

Responsibilities of the Management Team

• Develop and promote an eSafety culture within the school community.
• Support the eSafety coordinator in their work.
• Make appropriate resources, training and support available to members of the school community to ensure they are able to carry out their roles with regard to eSafety effectively.
• Receive and regularly review eSafety incident logs and be aware of the procedure to be followed should an eSafety incident occur in school.
• Take ultimate responsibility for the eSafety of the school community.

Responsibilities of the eSafety Coordinator

• Promote an awareness and commitment to eSafety throughout the school.
• Be the first point of contact in school on all eSafety matters.
• Create and maintain eSafety policies and procedures, with the support of other members of staff.
• Develop an understanding of current eSafety issues, guidance and appropriate legislation.

• Ensure that eSafety education is embedded across the curriculum.
• Ensure that eSafety is promoted to parents and carers.
• Liaise with appropriate staff in school, the local authority, the local safeguarding children's board and other relevant agencies as appropriate.
• Monitor and report on eSafety issues to the SMT as appropriate
• Ensure an eSafety incident log is kept up-to-date.

Responsibilities of Teachers and Support Staff

• Read, understand and help promote the school's eSafety policies and guidance.
• Read, understand and adhere to the school staff AUP.
• Develop and maintain an awareness of current eSafety issues and guidance.
• Model safe and responsible behaviours in your own use of technology.
• Embed eSafety messages in learning activities where appropriate.
• Supervise pupils carefully when engaged in learning activities involving technology.
• Be aware of what to do if an eSafety incident occurs.
• Maintain a professional level of conduct in their personal use of technology at all times.

Responsibilities of Technical Staff employed by the Local Authority

• Read, understand and adhere to the school staff AUP.
• Support the school in providing a safe technical infrastructure to support learning and teaching.
• Support the security of the school ICT system.
• Report any eSafety-related issues that come to your attention to the eSafety coordinator.
• Maintain a professional level of conduct in their personal use of technology at all times.

Responsibilities of Pupils

• Read, understand and adhere to the school pupil AUP.
• Help and support the school in creating eSafety policies and practices; and adhere to any policies and practises the school creates.

Responsibilities of Parents and Carers

• Help and support your school in promoting eSafety.
• Read, understand and promote the school pupil AUP with your children.
• Take responsibility for learning about the benefits and risks of using the Internet and other technologies that your children use in school and at home.
• take responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies
• Discuss eSafety concerns with your children, show an interest in how they are using technology, and encourage them to behave safely and responsibly when using technology.
• Model safe and responsible behaviours in your own use of technology.
• Consult with the school if you have any concerns about your children's use of technology.

Responsibilities of Governing Body

• Read, understand, contribute to and help promote the school's eSafety policies and guidance.
• Support the work of eSafety in school in promoting and ensuring safe and responsible use of technology in and out of school, including encouraging parents to become engaged in eSafety activities.
• Ensure appropriate funding and resources are available for the school to implement the eSafety strategy.

Responsibilities of Visiting Users

• Read, understand and adhere to the school staff AUP and report any eSafety issues.

Learning and Teaching

We believe that the key to developing safe and responsible behaviours online, not only for pupils but everyone within our school community, lies in effective education. We know that the Internet and other technologies are embedded in our pupils' lives not just in school but outside as well, and we believe we have a duty to help prepare our pupils to safely benefit from the opportunities the Internet brings.

• We will provide specific eSafety-related lessons in specific year groups as part of the ICT and PSHCE curriculum.
• We will celebrate and promote eSafety through assemblies.
• We will discuss, remind or raise relevant eSafety messages with pupils routinely wherever suitable opportunities arise; including the need to protect personal information, consider the consequences their actions may have on others, the need to check the accuracy and validity of information they use, and the need to respect and acknowledge ownership of digital materials.
• We will remind pupils about their responsibilities through an end-user AUP which every pupil will sign and will be displayed throughout .
• Staff will model safe and responsible behaviour in their own use of technology during lessons.

How parents and carers will be involved

We believe it is important to help all our parents develop sufficient knowledge, skills and understanding to be able to help keep themselves and their children safe. To achieve this we will:
• include eSafety as part of an annual parent meeting
• include useful links and advice on eSafety in newsletters and on our school website
• ensure a copy of the eSafety policy is easily accessible

Managing ICT Systems and Access

The school will be responsible for ensuring that access to the ICT systems is as safe and secure as reasonably possible.
• Servers and other key hardware or infrastructure will be located securely.
• Servers, workstations and other hardware and software will be kept updated as appropriate.
• Virus protection is installed on all appropriate hardware, and will be kept active and up-to-date.
• The school will agree which users should and should not have Internet access, and the appropriate level of access and supervision they should receive.
• All users will sign an end-user Acceptable Use Policy (AUP) provided by the school, appropriate to their age and access. Users will be made aware that they must take responsibility for their use of, and behaviour whilst using, the school ICT systems, and that such activity will be monitored and checked.
• At KS1 pupils will access the Internet using a class log-on, which the teacher supervises. All Internet access will be by working alongside a member of staff, or if working independently a member of staff will supervise at all times.
• At KS2 pupils will access the Internet using an individual log-on, which they will keep secure. Internet access will be supervised by a member of staff.
• Members of staff will access the Internet using an individual/class log-on, which they will keep secure. They will ensure they log-out after each session, and not allow pupils to access the Internet through their log-on. They will abide by the school AUP at all times.
• Any administrator or master passwords for school ICT systems should be kept secure and available to at least two members of staff.
• The school will take all reasonable precautions to ensure that users do not access inappropriate material. However it is not possible to guarantee that access to unsuitable material will never occur.
• The school will regularly audit ICT use to establish if the eSafety policy is adequate and that the implementation of the eSafety policy is appropriate. We will regularly review our Internet access provision, and review new methods to identify, assess and minimize risks.

Filtering Internet access

• The school uses a filtered Internet service. The filtering is provided through YHGfL.
• If users discover a website with inappropriate content, this should be reported to amember of staff who will inform the eSafety coordinator.
• If users discover a website with potentially illegal content, this should be reported immediately to the eSafety coordinator. The school will report this to appropriate agencies including the filtering provider, LA, Internet Watch Foundation (IWF) or Child Exploitation and Online Protection Centre (CEOP).
• Filtering and other security systems will be reviewed to ensure they meet the needs of all users.

Learning technologies in school

	Pupils	Staff
Personal mobile phones brought into school	Allowed with permission	Allowed
Mobile phones used in lessons	Not allowed	Allowed at certain times (e.g. educational visits)
Mobile phones used outside of lessons	Not allowed	Allowed at certain times
Taking photographs or videos on personal equipment	Not allowed	Not allowed
Taking photographs or videos on school devices	Allowed with supervision	Allowed
Use of hand-held devices such as PDAs, MP3 players or personal gaming consoles	Allowed with supervision	Allowed at certain times
Use of personal email addresses in school	Not allowed	Not allowed
Use of school email address for personal correspondence	Not allowed	Not allowed
Use of online chat rooms	Not allowed	Not allowed
Use of instant messaging services	Not allowed	Allowed at certain times
Use of blogs, wikis, podcasts or social networking sites	Not allowed	Not allowed
Use of video conferencing or other online video meetings	Allowed with supervision	Allowed

Using e-mail

• Staff and pupils should use approved e-mail accounts allocated to them by the school, and be aware that their use of the school e-mail system will be monitored and checked.
• Classes will be allocated an individual e-mail account for use by pupils within that class, under supervision of the class teacher.
• Pupils will be reminded when using e-mail about the need to send polite and responsible messages, about the dangers of revealing personal information, about the dangers of opening e-mail from an unknown sender, or viewing/opening attachments.
• Pupils are not permitted to access personal e-mail accounts during school.
• Any inappropriate use of the school e-mail system, or the receipt of any inappropriate messages by a user, should be reported to a member of staff immediately.

Using images, video and sound

• We will remind pupils of safe and responsible behaviours when creating, using and storing digital images, video and sound. We will remind them of the risks of inappropriate use of digital images, video and sound in their online activities both at school and at home.
• Digital images, video and sound will only be created using equipment provided by the school or a safe/reliable source.
• Staff and pupils will follow the school policy on creating, using and storing digital resources.
• In particular, digital images, video and sound will not be taken without the permission of participants; images and video will be of appropriate activities and participants will be in appropriate dress; full names of participants will not be used either within the resource itself, within the file-name or in accompanying text online; such resources will not be published online without the permission of the staff/pupils involved.
• If pupils are involved, relevant parental permission will also be sought before resources are published online.

Using video conferencing and other online video meetings

We use video conferencing to enhance the curriculum by providing learning and teaching activities that allow pupils to link up with people in other locations and see and hear each other. However, we will ensure that staff and pupils take part in these opportunities in a safe and responsible manner.

• All video conferencing activity will be supervised by a suitable member of staff.
• Pupils will not operate video conferencing equipment, or answer calls, without permission from the supervising member of staff.
• Video conferencing equipment will be switched off and secured when not in use/online meeting rooms will be closed and logged off when not in use.
• Pupils will be given appropriate user rights when taking part in an online meeting room. They will not have host rights or the ability to create meeting rooms.
• Video conferencing should not take place off school premises without the permission of the head teacher.
• Parental permission will be sought before taking part in video conferences.
• Permission will be sought from all participants before a video conference is recorded. Video conferences should only be recorded where there is a valid educational purpose for reviewing the recording. Such recordings will not be made available outside of the school.

Using mobile phones

• Pupils will be provided with school mobile phones to use in specific learning activities under the supervision of a member of staff. Such mobile phones will be set up such that only those features required for the activity will be enabled.

Using new technologies

• As a school we will keep abreast of new technologies and consider both the benefits for learning and teaching and also the risks from an eSafety point of view.
• We will regularly amend the eSafety policy to reflect any new technology that we use, or to reflect the use of new technology by pupils which may cause an eSafety risk.

Protecting personal data

• We will ensure personal data is recorded, processed, transferred and made available according to the Data Protection Act 1998.
• Staff will ensure they properly log-off from a computer terminal after accessing personal data.
• Staff will not remove personal or sensitive data from the school premises without permission of the headteacher, and without ensuring such data is kept secure.

The school website and other online content published by the school

• The school website will not include the personal details, including individual e-mail addresses or full names, of staff or pupils.
• A generic contact e-mail address will be used for all enquiries received through the school website.
• All content included on the school website will be approved by the head teacher before publication.
• Staff and pupils should not post school-related content on any external website without seeking permission first.

Dealing with eSafety incidents

In most situations, where a member of staff is made aware of a possible eSafety incident, they should inform the eSafety coordinator or headteacher who will then use the school's agreed procedure to respond in the most appropriate manner. See appendix 1 and 2.

Appendices

Appendix 1

Staff Procedures Following Misuse by Staff

The Headteacher will ensure that these procedures are followed, in the event of any misuse of the Internet, by an adult:

A. An inappropriate website is accessed inadvertently:
Report website to the e-Safety Leader if this is deemed necessary.
Contact the helpdesk filtering service for school and LA/RBC so that it can be added to the banned or restricted list. Change Local Control filters to restrict locally.
Check the filter level is at the appropriate level for staff use in school.

B. An inappropriate website is accessed deliberately:
Ensure that no one else can access the material by shutting down.
Log the incident. Report to the Headteacher and e-Safety Leader immediately.
Headteacher to refer back to the Acceptable Use Rules and follow agreed actions for discipline. Inform the LA/RBC filtering services as with A.

C. An adult receives inappropriate material.
Do not forward this material to anyone else – doing so could be an illegal activity.
Alert the Headteacher immediately. Ensure the device is removed and log the nature of the material. Contact relevant authorities for further advice e.g. police.

D. An adult has used ICT equipment inappropriately:
Follow the procedures for B.

E. An adult has communicated with a child or used ICT equipment inappropriately:
Ensure the child is reassured and remove them from the situation immediately, if necessary. Report to the Headteacher and Designated Person for Child Protection immediately, who should then follow the Allegations Procedure and Child Protection Policy from Section 12, LSCBN. Preserve the information received by the child if possible and determine whether the information received is abusive, threatening or innocent. Once Procedures and Policy have been followed and the incident is considered innocent, refer to the Acceptable Use Rules for Staff and Headteacher to implement appropriate sanctions. If illegal or inappropriate misuse is known, contact the Headteacher or Chair of Governors (if allegation is made against the Headteacher) and Designated Person for Child Protection immediately and follow the Allegations procedure and Child Protection Policy. Contact CEOP (police) as necessary.

F. Threatening or malicious comments are posted to the school website or learning platform (or printed out) about an adult in school:
Preserve any evidence. Inform the Headteacher immediately and follow Child Protection Policy as necessary. Inform the LA and e-Safety coordinator so that new risks can be identified. Contact the police or CEOP as necessary.

G. Where staff or adults are posted on inappropriate websites or have inappropriate information about them posted this should be reported to the Headteacher.

Appendix 2

Staff Procedures Following Misuse by Children and Young People

The Headteacher will ensure that these procedures are followed, in the event of any misuse of the Internet, by a child or young person:

A. An inappropriate website is accessed inadvertently:
Reassure the child that they are not to blame and praise for being safe and responsible by telling an adult. Report website to the e-Safety coordinator if this is deemed necessary. Contact the helpdesk filtering service for school so that it can be added to the banned list or use Local Control to alter within your setting. Check the filter level is at the appropriate level for use in school.

B. An inappropriate website is accessed deliberately:
Refer the child to the Acceptable Use Rules that were agreed. Reinforce the knowledge that it is illegal to access certain images and police can be informed. Decide on appropriate sanction. Notify the parent/carer. Inform LA as above.

C. An adult or child has communicated with a child or used ICT equipment inappropriately:
Ensure the child is reassured and remove them from the situation immediately. Report to the Headteacher and Designated Person for Child Protection immediately. Preserve the information received by the child if possible and determine whether the information received is abusive, threatening or innocent. Contact CEOP (police) as necessary.

D. Threatening or malicious comments are posted to the school website or learning platform about a child in school:
Preserve any evidence. Inform the Headteacher immediately. Inform the LA and eSafety coordinator so that new risks can be identified. Contact the police or CEOP as necessary.

E. Threatening or malicious comments are posted on external websites about an adult in the school or setting:
Preserve any evidence. Inform the Headteacher immediately.

N.B. There are three incidences when you must report directly to the police.

- Indecent images of children found.
- Incidents of 'grooming' behaviour.
- The sending of obscene materials to a child.

CEOP advice is to turn off the screen, secure the machine and contact the police for further instructions if an indecent image is found.
They will advise on how to deal with the machine, if they are unable to send out a forensics team immediately. If in doubt, do not power down the machine.
Grabbing a screenshot is not a technical offence of distribution, but of 'making' an image.
• www.iwf.org.uk will provide further support and advice in dealing with offensive images on-line.

Appendix 3

Pupil Acceptable Use Policy

You can use the computers and other devices in school to access the Internet to help you with your learning. These rules will help make sure the Internet is a safe and fun place for everyone in school. You will need to agree to follow these rules whenever you access the Internet at school.

• I will only use the computers and other devices for school work and homework
• I will ask permission from a member of staff before using the Internet
• I will only visit websites to help me with schoolwork or homework, or that my teacher has said I can go on
• I will only send messages to people I know, or my teacher has agreed to
• The messages I send and the work I do will be polite and responsible, and not contain anything that might upset someone else
• I will only open attachments in messages I receive, or download a file, if I trust the person who sent it or the website it is from, and I've checked with my teacher that it is saf.
• I will only use equipment or files I bring from home, such as my mobile phone or files on a USB stick, if the school lets me, and only use them for activities the school agrees to
• I will keep my username and password safe by not telling anyone else
• I will not change any settings on the computers and other devices I use at school
• I will not install or delete any software on the computers and other devices I use at school
• I will only change or delete my own files
• I will only look at other people's files or messages with their permission
• I will not give away any of my personal information, or the personal information of people I know, over the Internet. This includes my full name, address, phone numbers, photographs and videos of me and my friends, or the name of my school unless my teacher has checked it is safe
• I will never arrange to meet anyone that I have never met in real-life before, unless my parent or teacher has given me permission and I take a responsible adult with me
• If I see or receive anything that is unpleasant, or makes me feel uncomfortable or upset, I will use the 'Hector Protector' button and report it to a member of staff immediately
• If something happens whilst using a computer or school device, and I am not sure what I should do next, I will ask a member of staff to help me
• Finally:
• I understand that the school may check my computer files, the Internet sites I visit, the messages I send and anything else I do to make sure I am keeping myself and others safe
• I understand that if I do not follow these rules and other guidance from the school as best as I can then I may not be allowed to use the Internet or any of the school's computers

Appendix 4

Staff and other adults in school AUP

These statements are designed to ensure staff and other adults in school are aware of
their professional responsibilities when using the ICT systems provided. All staff should
follow the guidelines at all times. You are responsible for your behaviour and actions when accessing the Internet at school, whether on your own or school equipment, and
when using school ICT equipment at other locations such as your home.

• Any use of school ICT systems will be for professional purposes as agreed by the school senior management team
• Usernames, passwords and other logon details should be kept secure and not revealed to anyone else. Care should be taken to ensure you logout when not actively using the ICT systems. You should not allow an unauthorised person to access the school ICT systems, e.g. by logging in for them.
• Any online activity should not harass, harm, offend or insult other users.
• You will not search for, download, upload or forward any content that is illegal, or that could be considered offensive by another user. If you accidentally encounter such material you should follow your school's procedure and report this immediately.
• You should not download or install any hardware or software without permission. If you have responsibility for installing software you should be confident it is adequately licensed and appropriate for educational use.
• Ensure that any files on removable media (e.g. USB drives, CDs) are free from viruses and other malware before use and that such devices are not used for carrying sensitive data or details of pupils, parents or other users without suitable security and without permission from the Headteacher.
• Any electronic communications should be related to schoolwork only. It is not acceptable to contact pupils using personal equipment or personal contact details including your own mobile phone or through your personal social network profiles.
• Any online activity, including messages sent and posts made on websites, and including activity outside of school, should not bring your professional role or the name of the school into disrepute.
• Any still or video images of pupils and staff should be for professional purposes only.
• You will not give out your personal details, or the personal details of other users, to pupils or parents or on the Internet. In particular you should ensure your home address, personal telephone numbers and email accounts are not shared with children, young people or parents.
• You should ensure that any personal or sensitive information you use or access (e.g. SIMS data, assessment data) is kept secure and used appropriately.
• Personal or sensitive information should only be taken off-site if agreed with the Headteacher, and steps should be taken to ensure such data is secure.
• You should respect intellectual property and ownership of online resources you use in your professional context, and acknowledge such sources if used.

• You should support and promote the school eSafety Policy, and promote and model safe and responsible behaviour in pupils when using ICT to support learning and teaching
• Finally: You understand that your files, communications and Internet activity may be monitored and checked at all times to protect your own and others' safety, and action may be taken if deemed necessary to safeguard yourself or others. If you do not follow all statements in this AUP and in other school policies you may be subject to disciplinary action in line with the school's established disciplinary procedures.