KILLINGHALL CE PRIMARY SCHOOL

Acceptable Use Statement

ICT in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.
Information and Communications Technology covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- E-mail, Instant Messaging and chat rooms
- Social Media, including Facebook, Twitter and Instagram
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices with web functionality
- Gaming, especially online
- Learning Platforms and Virtual Learning Environments
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies and that some have minimum age requirements, usually 13 years.

At Killinghall CE Primary School we understand the responsibility to educate our pupils on eSafety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Schools hold personal data on learners, staff and other people to help them conduct their day-to-day activities. Some of this information is sensitive and could be used by another person or criminal organisation to cause harm or distress to an individual. The loss of sensitive information can result in media coverage, and potentially damage the reputation of the school. This can make it more difficult for the school to use technology to benefit learners.

Everybody in the school has a shared responsibility to secure any sensitive information used in their day to day professional duties and even staff not directly involved in data handling are made aware of the risks and threats and how to minimise them.

Both this policy and the Acceptable Use Agreement (for all staff, governors, visitors and pupils) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, mobile devices, webcams, whiteboards, cameras, digital video equipment, etc); and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobile phones and other mobile devices).

The Aims of the Acceptable Use Policy are to:-

Allow all users access to school ICT resources and use of the Internet for educational purposes.
Provide a mechanism by which staff and pupils are protected from Internet sites, information, and individuals that would undermine the principles and aims of the school.
Provide rules which are consistent, and in agreement with the Data Protection Act 1984, Computer Misuse Act 1990 and other legislation relevant to the use of computers and electronic data in schools.
Provide rules that are consistent with the acceptable procedures commonly used on the Internet, including those associated with netiquette.
Provide rules relating to the use of computers and ICT facilities in school, which are consistent with the general policies of the school.

General Internet use and Consent

Pupils who are to have access to the internet must understand the basic conventions and navigation techniques before going online and accessing material.
Pupils must have returned a signed consent form before being allowed to use the ICT facilities that involve accessing the internet.
The use of the names of pupils or photographs of pupils for websites will require written permission from parent(s)/guardian(s) included on the use of photos consent form. If a picture is placed on the website the child's full name will not be displayed.

Pupils must not use the school ICT facilities without the supervision of a member of staff. Although use of the ICT facilities and access to the Internet will be supervised, and all possible measures will be taken (including the use of filtering and firewall), Killinghall CE Primary cannot accept liability for the accessing of inappropriate materials or any consequences of internet access.

If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Headteacher immediately who will, in turn, record the address and report it to NYCC Schools ICT.
Pupils are aware that they must only access those services they have been given permission to use.

Staff and pupils are made aware that the use of computer systems without permission or for inappropriate purposes is a criminal offence (Computer Misuse Act 1990)
Staff and Governors must agree to and sign the Acceptable Use Agreement (see appendix) each year.

Log in and Passwords

Pupils and staff must not disclose any password or login name given to anyone, or allow anyone else to use a personal account.
Pupils and staff must not attempt to gain access to the school network or any Internet resource by using someone else's account name or password.
Staff and pupils must ensure terminals or lap tops are logged off (or hibernated) when left unattended.
Adult users are expected to be in charge of their own areas on the network. Passwords are therefore set for each user.
We recommend that passwords are changed frequently. Passwords should be over 4 characters and should contain letters, numbers and symbols. They should not contain spaces.

General Safety and Risk Assessment

The consumption of food or drink is forbidden whilst using a computer. It is hazardous to the equipment and to individuals.
Users must treat with respect equipment and services in school and at other sites accessed through school facilities, and are subject to regulations imposed by the respective service providers. Malicious action will result in immediate suspension from use of the school facilities.
Staff are responsible for sharing the safety issues with their pupils.

Cyber Bullying

The experience of being cyber bullied can be very painful for those who are the targets. Adults need to help children and young people prepare for the hazards of using technology while promoting learning and social opportunities. Some forms of cyber bullying are different from other forms:

- Through various media children can be cyber bullied 24 hours a day.
- People who cyber bully may attempt to remain anonymous.
- Anyone of any age can cyber bully.
- Some instances of cyber bullying may be unintentional – such as a text sent as a joke or an email to the wrong recipient.

Prevention

We recognise that the best way to deal with cyber bullying is to prevent it from happening in the first place. By embedding good, safe ICT practice into all our teaching and learning, incidents can be avoided. Anti Bullying weeks highlight this issue. We recognise we have a shared responsibility to prevent incidents of cyber bullying.

Understanding Cyber bullying

The school community is aware of the definition of cyber bullying and the impact cyber bullying has. Staff receive guidance and review the Anti-Bullying and Acceptable Use Policies regularly. Children are taught how to recognise cyber bullying and their responsibilities to use ICT safely. ICT safety is integral to teaching and learning practice in the school.

As with other forms of bullying, the Headteacher keeps records of cyber bullying. Incidents of cyber bullying will be followed up using the same procedures as other forms of bullying.

E-Safety

Children and staff are reminded of E-Safety Codes of Conduct at the start of each academic year. Every year an ‘esafety day’ will be held in school.

Any work or activity on the Internet must be directly related to schoolwork. Private use of the Internet (including social networking sites) in school is strictly forbidden.

Staff are discouraged from being members of social networking sites. However, if staff are members they are reminded of the necessity to keep their profiles secure and to avoid contact with persons (particularly parents/pupils or ex-pupils) related to the school. Staff are reminded that any action or comment that brings the school or colleagues into disrepute or compromises pupil or staff confidentiality will be classed as a disciplinary matter.

School Network and Pupil Files

Always respect the privacy of files of other users. Do not enter the file areas of other users without obtaining their permission first. Files to be shared should be saved to the shared area. Pupils can access and save work to their own class log-on through the server.

Do not modify or delete the files of other users on the shared areas without obtaining permission from them first.

Storage space on the network is limited. All users are requested to ensure that old unused files are removed from their area at the end of each academic year. Users unsure of what can be safely deleted should ask their teacher for advice.

Users accessing software or any services available through school facilities must comply with licence agreements or contracts relating to their use and must not alter or remove copyright statements. Some items are licensed for educational or restricted use only.

Security Guidelines

Backups

Files stored on the network are backed up every evening. This means files can be restored if deleted or lost in error. However, if you create and delete files on the same day then a backup will not be available to restore. Back ups are kept securely.

Save Regularly

It is very important to save work regularly (approx. every 10 minutes). The network is very reliable but problems do occur i.e. programs crash, power failures. If work is saved regularly and a PC or the network does fail for any reason, only the work done since the last save will be lost.

Use your Network Area

Always ensure that files are saved to your network area, NOT on the local hard drive. This will ensure that your work is backed up and can be retrieved in the event of a hardware failure or theft.

Staff should only use their mobile phones at appropriate times of the day. These are break times. During the school day their mobiles should be turned off or set to silent. Staff must not use personal mobile devices or cameras to take images of pupils or staff.

No pupils are permitted to have a mobile device in school either on their person, or in their bag. With written permission from the class teacher and parental consent plus parental responsibility, a mobile device may be allowed in school. It must be handed in to the class teacher or to the school office for safe keeping. Any pupil who is seen with a mobile device during the school day will have it removed from them to be collected at the end of the school day. The device will be stored securely.

Sanctions

If pupils break the rules as laid down by this policy they will lose temporary or permanent use of the school systems. Parents will be informed.
If staff break the rules as laid down by this policy they will lose temporary or permanent use of the school systems and will be subject to disciplinary proceedings. If the law has been broken the police will be informed and the school will assist the police with any prosecution.

2020

Date for Review: Sept 2021

KILLINGHALL CE 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 ICT and the related technologies such as hardware, software, internet, email, Learning Platforms, web2 technologies, mobile devices, cameras 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, secure school 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.
- Should not use school information systems or resources (eg cameras, laptops, memory devices) for personal purposes without specific permission from the Headteacher; they should only be used for professional purposes.
- 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. Any such device must be encrypted.
- Should ensure that personal data (such as data held on SIMS) 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.
- Should ensure that their use of web 2 technologies, including social networking sites, such as Facebook, Bebo, Myspace, Instagram, 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 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 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…………………………………..

Killinghall CE Primary School Pupil Acceptable Use

ICT including the internet, e-mail and mobile technologies has become an important part of learning in our school. We expect all children to be safe and responsible when using any ICT.

The statutory curriculum requires pupils to learn how to locate, retrieve and exchange information using ICT. Consequently, in delivering the curriculum teachers need to plan to integrate the use of ICT and web based resources including e-mail to enrich learning activities. Effective internet use is an essential life skill.

Access to the school's ICT network and use of ICT facilities owned by the school, including access to the Internet, are conditional on observance of the following Acceptable Use Policy. All staff in school also have to comply with the NYCC acceptable use policy.

Please read and discuss these eSafety rules with your child and return the slip at the bottom of this page.

Primary Pupil Acceptable Use
Agreement / eSafety Rules

- I will only use ICT in school for school purposes.
- I will only use my class logon and password.
- I will only open/delete my own files.
- I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.
- I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will tell my teacher immediately.
- I will not give out my own details such as my name, phone number or home address. I will not arrange to meet someone unless this is part of a school project approved by my teacher and a responsible adult comes with me.
- I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community
- I know that my use of ICT can be checked and my parent/carer contacted if a member of school staff is concerned about my eSafety.

✂

ICT Acceptable use

We have discussed this and ………………………………….........(child name) agrees to follow the eSafety rules and to support the safe use of ICT at Killinghall CE Primary School.

Parent/ Carer Signature …….……………………….……………………….

Class …………………………………. Date ………………………………