Killisick Junior School

ICT Acceptable Use and e-Safety Policy

L Rotherham
Updated March 2023

ICT Acceptable Use and e-Safety Policy

General Statement

This e-safety policy has been developed and agreed by the Computing coordinator, Headteacher, Senior Leaders and school governors. The implementation of this policy will be monitored by the coordinator and Headteacher and will be monitored at regular intervals. The e-safety policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of technologies, new threats to e-safety or incidents that have taken place. Should serious e-safety incidents take place, the following external persons/agencies should be informed: Local Authority manager, Local Authority safeguarding officer or Police as appropriate.

Permission to use the School's ICT facilities is given subject to agreement by users to the terms of use set out in this policy. Failure to comply fully at any time may be deemed to have broken the rules of acceptable use and permission to use the system suspended. The 'Computer Misuse *Act 1990'* and 'Data Protection *Act 1998'* also apply in law. Users should also be mindful of current copyright legislation. Serious abuse may be construed as a criminal act and *may result in disciplinary procedures.*

Scope of the Policy

The policy applies to:

- *All permanent, temporary and casual staff working at the school*
- *Pupils*
- *Students or volunteers*
- *Governors*
- *Parents/Carers*
- *Consultants, contractors, agency staff and others working at the school, including those affiliated with third parties.*

The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students/ pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place outside of the school but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data (see appendix for template policy). In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/ carers of incidents of inappropriate e-safety behaviour that take place out of school.

Roles and Responsibilities

The following section outlines the e-safety roles and responsibilities of individuals and groups within the school.

Governors:

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about e-safety incidents and monitoring reports. As part of Child Protection,

Governors will be responsible for:
• monitoring of e-safety incidents. All attempted breeches will be documented every term in the headteacher's report to governors. The chair of governors will also monitor this during safeguarding visits.
• monitoring of filtering / change control logs

Headteacher/Senior Leaders:

- The Headteacher has a duty of care for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to the E-Safety Co-ordinator.
- The Headteacher and Deputy Headteacher should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff. (see flow chart on dealing with e-safety incidents – included in a later section – "Responding to incidents of misuse" and relevant Local Authority HR / other relevant body disciplinary procedures).
- The Headteacher/ Senior Leaders are responsible for ensuring that the E-Safety Coordinator and other relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.
- The Headteacher/ Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Senior Leadership Team will receive regular monitoring reports from the E-Safety Co-ordinator.

E-Safety Coordinator:

• takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents
• ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
• provides training and advice for staff
• liaises with the Local Authority / relevant body
• liaises with school technical staff
• receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments
• discuss current issues, review incident logs and filtering / change control logs
• reports regularly to Senior Leadership Team

Network Manager / Technical staff:

It is the responsibility of the school to ensure that the managed service provider carries out all the e-safety measures that would otherwise be the responsibility of the school technical staff, as suggested below. It is also important that the managed service provider is fully aware of the school e-safety policy and procedures.

The Network Manager / Technical Staff:

• that the school's technical infrastructure is secure and is not open to misuse or malicious attack

• that the school meets required e-safety technical requirements and any Local Authority / other relevant body E-Safety Policy / Guidance that may apply.
• that users may only access the networks and devices through a properly enforced password protection policy
• the filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
• that they keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant

Teaching and Support Staff

are responsible for ensuring that:
• they have an up to date awareness of e-safety matters and of the current e-safety policy and practices
• they have read, understood and signed the Staff Acceptable Use Policy
• In line with recent 'PREVENT' training, they understand how to act on concerns and why it is important to do so.
• they report any suspected misuse or problem to the Headteacher / Senior Leader ;
• all digital communications with students / pupils / parents / carers should be on a professional level and only carried out using official school systems
• e-safety issues are embedded in all aspects of the curriculum and other activities
• students/ pupils understand and follow the e-safety and acceptable use policies
• students/ pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
• they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices
• in lessons where internet use is pre-planned students / pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Child Protection/ Safeguarding Designated Person

should be trained in e-safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:
• sharing of personal data
• access to illegal / inappropriate materials
• inappropriate on-line contact with adults / strangers
• potential or actual incidents of grooming
• cyber-bullying
These issues will be covered in the school safeguarding policy

All breaches will be reported to the DSL who will report to governors every term at the full governor's meeting.

Computer equipment

- Staff are responsible for keeping in good order the class laptop loaned to them and for ensuring that any fault or damage found on equipment is reported.
- No software should be copied onto or removed from any computer hardware without the required software license.

Passwords

- Users must use ONLY their own valid usernames and personal passwords to log on to the school Network or email. The password will not be divulged to anyone, at any time! Users must immediately report to the *Headteacher and* ICT coordinator, if at any time their access to any of these resources is compromised. Any attempt at or actual use of another user's identity is an infringement of the 'Computer Misuse Act'.

- Laptops and PCs must never be left unattended when signed-on to the system. If it is necessary to deal with an immediate concern the computer must be locked using the windows software facility by pressing Ctrl+Alt+Delete and choosing lock computer.
- Passwords must not be disclosed to unauthorised persons.
- Our current password policy is as follows:

  Staff will be allocated a username giving them access to their own area and staff shared resources. If staff are aware of, or are concerned that their password security has been compromised, they must immediately inform the network manager;

  Pupils will be issued a log in for their year group. Pupils have no access rights to confidential data.

Use of Equipment

- All computer facilities (ICT suite, laptops and PCs) are made available to staff to carry out their professional duties. Use of the equipment at home for personal use, providing internet safety measures are in place is acceptable. The equipment should be kept safe and made secure when not being used in a secure and locked environment.
- Repairs and disposal of equipment concerns should be passed through to the ICT coordinator who has responsibility in ensuring the equipment is made good and disposed of appropriately in accordance with current statutory regulations.
- Staff may be issued with a Laptop on loan.
- The use of ICT equipment must be for educational purposes only. No attempt must be made by a pupil to use a personal computer or laptop to connect to the school Network unless authorised to do so.

Use of the School Network

- Under no circumstances will files other than non-executable files produced by the pupils themselves be allowed to be copied onto the Network. Only sensible naming of files will be tolerated. Deliberate unauthorised access to, copying alteration, or interference with computer programs or data is not allowed. Users will only have access to those folders specifically allocated to them. This includes a pupil folder area and common resources used for teaching. Under NO circumstance must attempts be made to access any other areas on the system.
- If any unusual desktop or application appears, it is the direct responsibility of the user to alert the ICT coordinator. Only those applications where a start menu or a desktop shortcut is provided are authorised. Users will only ever log on to a single station at one time and ensure it is reset correctly before they leave.
- Pupils may only enter a Computer Suite with the permission of a member of staff. No unsupervised access will be allowed. Pupils will use computers designated for pupil use only. No pupil will attempt to use any machine marked or obviously for staff use or in a non-designated area.
- No damage should be made to the computers, associated equipment or suites in general. Machines will not be moved, nor should any be switched on or off without permission. All equipment is to be handled in an appropriate manner, such as to maintain it in the best possible condition. No food, drink, sweets nor any other substance likely to be detrimental is ever to be brought into the IT suites, whether in bags or openly. The machine, mouse, keyboard, chair etc. are to be replaced in a tidy fashion after use.
- No attempt is ever to be made to access internal components of machines, nor introduce foreign objects. Any physical defects or errors must be reported immediately to a member of staff. Anyone proven to have intentionally damaged equipment may well be reported for criminal damage and be obliged to compensate financially for any loss.

- Pupils must obtain permission from the teacher or teaching assistant in charge of the class to print their work.
- No information or data is to be sent using any part of the Network and the access granted here from within or outside of the system, to any other user, which may be construed to give cause for concern or offence to that user, be racist, sexist, etc., be in general bad taste, bring the reputation of the school into disrepute, or be in any way unlawful. Any form of 'cyber' bullying will not be tolerated.

Use of Internet based services

- The Network and ICT services provided by the school remains the intellectual property of the school and no right of privacy is allowed. Folders and email accounts are all open to scrutiny by appropriate staff. Email is available via private accounts on the internet, i.e. hotmail, and staff may, if they choose, use it for personal correspondence but should be aware that the school reserves the right to audit the account.
- Internet access is provided for genuine educational use only. There is no absolute right of access granted to commercial sites or those that might have questionable content.
- ICT will use filtering to block sites which have potentially harmful or questionable content. However, new sites appear continually – just because a site may be accessible, it does NOT imply that the school approve of the content. Such lapses must be immediately reported. Common sense, good taste and judgment must always be exercised.
- Copyright laws must always be respected when using Internet material.
- No programme or tool or device of any description is to be run, remotely or otherwise, which may compromise the network in any way, whatsoever.
- When using School laptops staff must ensure that no confidential data is stored without file password protection. The same policy applies to all portable storage devices.

School Rules for Pupils using ICT

- No food or drink is to be brought into IT rooms.
- Equipment should never be moved or unplugged.
- You can only enter a computer room with permission and under the supervision of a member of staff.
- To print work the file must have been saved in your work space with an appropriate name. Permission from staff is required before printing.

Pupils are abusing the school network and internet facility if they:

- bypass the school filtering rules by using any website designed to allow unfiltered internet access;
- log on to the network or the internet using another person's username and password without permission;
- attempt to find out anyone else's username and password;
- view or navigate any website with inappropriate content, including social chatrooms, games and pornographic or offensive material;
- edit, delete or move another person's files or folders;
- tamper with the network settings in any way;
- introduce inappropriate or offensive material to any drive on the school network;
- introduce any software program that could corrupt, damage or modify the school network, including viruses;
- physically damage computer equipment;
- steal computer equipment.

If a pupil abuses the system, their parents will be informed about the abuse. The school will then decide to use a sanction that is deemed appropriate to the abuse.

If a pupil abuses the system more than once, it will be seen as a deliberate disregard for the school's policy. Parents will automatically be asked to come into school to discuss the abuse. Normal school sanctions will apply if material that pupils view or share causes harm (or has the potential to cause harm) to other pupils or staff in the school. These sanctions may include any consequence that the school decides is appropriate, including fixed-term exclusion.

Use of Internet or e-mail

- *Access to Internet or e-mail must be through an authorised user account and all use must be linked to this account;*
- *Users must immediately report to the Headteacher or the ICT Coordinator if they receive offensive e-mail;*
- *Users must only reveal details of themselves or others in e-mail or Internet communication, such as address or telephone number, where it is considered acceptable as part of legitimate school related activity;*
- *Users must protect their passwords at all times in accordance with the guidance above;*
- *Users must not put in an e-mail anything that they would not include in a formal letter or what they would be prepared to say verbally;*
- *Confidential information must not be sent in an e-mail unless protected and users must not assume that e-mail content is confidential;*
- *Users must be aware the school reserves the right to access messages sent over the e-mail system.*

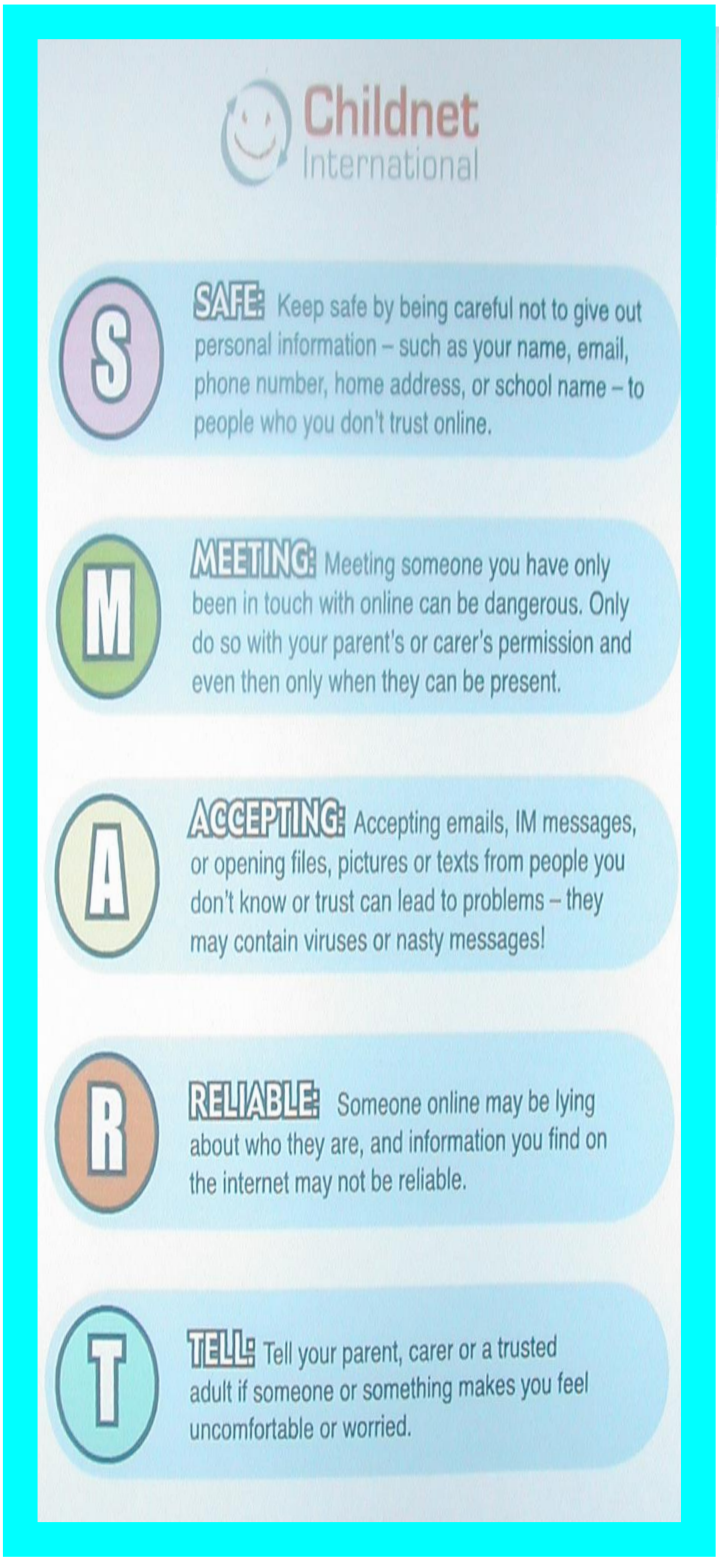
The School's Internet and e-mail system may not under any circumstances be used to transmit, search for, engage in, or access any communications or images which are:

- *Harassing – including but not limited to material relating to gender, race, sexual orientation, religion, disability and include insults and 'jokes';*
- *Discriminatory – material that might be considered discrimination by others;*
- *Copyright – unless specifically permitted;*
- *Criminal or Unlawful – material that is an offence or incitement to commit a criminal offence including fraud;*
- *Offensive or Insulting – material that might reasonably be expected to cause distress to others;*
- *Sexually inappropriate*
- *Racist;*
- *Commercial Activities – including offering services or merchandise for sale unless for the school's legitimate business;*
- *Disabling or damaging hardware, software or data;*
- *Downloading pirated software or data covered by the Data Protection Act 1998;*
- *Accessing peer-to-peer file sharing programs unless a school requirement;*
- *Corrupting or destroying other users' data;*
- *Violating the privacy of others;*
- *Interfering with the Internet or e-mail including corrupting data, propagation of computer viruses or causing network congestion i.e. spam;*
- *Using the Internet or e-mail for soliciting, representing personal opinions or revealing confidential information or in any other way that could reasonably be considered inappropriate.*

Online safety

With young children now accessing the internet at school and at home, it is important that children are made fully aware of the online safety issues. As a result, parents are to receive the Killisick leaflet 'Keeping Safe Online' to make them aware of the risks. Parents and teachers need to provide help and advice about being safe online. All staff received 'Prevent' training and are aware of the changing ways in which children are vulnerable, signs to look for and how to report concerns.

It is important not to inadvertently cause fear or anxiety; however it is important to ensure that children do understand the issues of personal safety online. We also use the five ***SMART*** rules for safety. The five ***SMART*** rules are summarised on the attached poster.



Childnet International

S **SAFE:** Keep safe by being careful not to give out personal information – such as your name, email, phone number, home address, or school name – to people who you don't trust online.

M **MEETING:** Meeting someone you have only been in touch with online can be dangerous. Only do so with your parent's or carer's permission and even then only when they can be present.

A **ACCEPTING:** Accepting emails, IM messages, or opening files, pictures or texts from people you don't know or trust can lead to problems – they may contain viruses or nasty messages!

R **RELIABLE:** Someone online may be lying about who they are, and information you find on the internet may not be reliable.

T **TELL:** Tell your parent, carer or a trusted adult if someone or something makes you feel uncomfortable or worried.

Information for Parents and Carers

Killisick Junior School

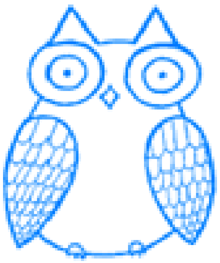
What can be done to help?

- Talk about safe internet usage
- Create parental controls
- Monitor usage
- Consider age restrictions
- Discuss what to do if children have problems online
- Have clear e-safety rules for devices at home
- Find out about the things children are using—it's safer if you understand it too.

Where can we go for help?

www.killisick.notts.sch.uk
www.kidsmart.org.uk
www.vodafone.com
www.kidscape.org.uk
www.childline.org.uk
www.beatbullying.org.uk
www.childnet-int.org
www.saferinternet.org.uk
For adult courses, visit www.ikeepsafe.org/parents

Killisick Junior School



Believe to Achieve and Succeed

Information for Parents and Carers

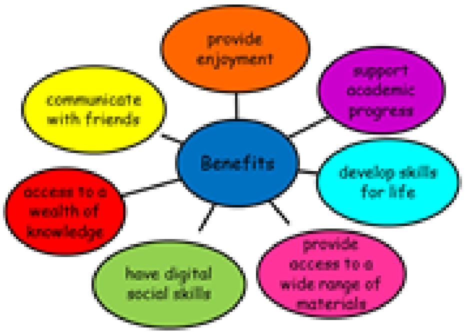
Keeping Safe Online

Believe to Achieve and Succeed

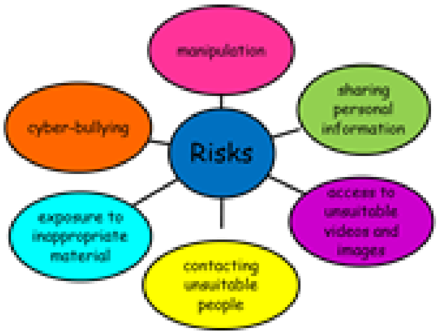
At school, we have been thinking about how we use technology today and all of the fantastic things we can do with it. Although it can provide countless positive outcomes, it is vital that our children understand the possible risks and what they need to do to keep safe online.

As a parent or carer, you play a vital role in ensuring that your child understands how to follow e-safety rules and keep safe. It is our job to provide children with the knowledge and understanding to use the internet safely and benefit from the opportunities it provides.

What are the benefits of using the internet?


Benefits
provide enjoyment
support academic progress
communicate with friends
develop skills for life
access to a wealth of knowledge
have digital social skills
provide access to a wide range of materials

What are the risks?


Risks
manipulation
sharing personal information
cyber-bullying
exposure to inappropriate material
access to unsuitable videos and images
contacting unsuitable people