Policy Title:	e-Safety (incl. Acceptable Use)
Policy Folder:	Pastoral
Last Review:	July 2018
Next Review:	July 2021
Led By:	IT Co-ordinator
Responsible Committee:	SD Committee

Introduction:

E-safety is defined as being safe from risks to personal safety and wellbeing when using all fixed and mobile devices that allow access to the internet, as well as those that are used to communicate electronically. This includes personal computers, laptops, mobile phones and gaming consoles such as Xbox, Playstation and Wii.

Safeguarding against these risks is not just an ICT responsibility, it is everyone's responsibility and needs to be considered as part of the overall arrangements in place that safeguard and promote the welfare of all members of the community, particularly those that are vulnerable.

Our E-safety Policy has been written by the school, involving all stakeholders and builds on best practice and government guidance. It relates to the latest version of DfE statutory guidance: **'Keeping Children Safe in Education'**.

Cyber-bullying by pupils will be treated as seriously as any other type of bullying and will be managed through our
Anti-bullying Policy and **Behaviour Policy**.

Understanding the risks of using the Internet and associated devices:

The internet is an essential element in 21st century life and ICT knowledge, now seen as an important life-skill, is vital to access life-long learning and employment. It is also important to recognise that the internet provides many benefits, not just to children, young people and vulnerable adults, but also to the professional work of staff.

E-safety covers the Internet but it also covers mobile phones and other electronic communications technologies. We know that some adults and young people will use these technologies to harm children. The harm might range from sending hurtful or abusive texts and emails, to enticing children to engage in sexually harmful conversations or actions online, webcam filming, photography or face-to-face meetings.

There is a 'duty of care' for any persons working with children and educating all members of the school community on the risks and responsibilities of E-safety falls under this duty. It is important that there is a balance between controlling access to the Internet and technology and allowing freedom to explore and use these tools to their full potential. This policy aims to be an aid in regulating ICT activity in school, and provide a good understanding of appropriate ICT use that members of the school community can use as a reference for their conduct online outside of school hours. E-safety is a whole-school issue and responsibility.

While acknowledging the benefits, it is also important to recognise that risk to safety and well-being of users is ever- changing as technologies develop. These can be summarised as follows:

Content

- Commercial (adverts, spam, sponsorship, personal information)
- Aggressive (violent/hateful content)
- Sexual (pornographic or unwelcome sexual content)
- Values (bias, racism, misleading info or advice)

Contact

- Commercial (tracking, harvesting personal information)
- Aggressive (being bullied, harassed or stalked)
- Sexual (meeting strangers, being groomed)
- Values (self-harm, unwelcome persuasions)

Conduct

- Commercial (illegal downloading, hacking, gambling, financial scams, terrorism)
- Aggressive (bullying or harassing another)
- Sexual (creating and uploading inappropriate material, including sexting)
- Values (providing misleading info or advice)

Much of the material on the internet is published for an adult audience and some is unsuitable for children and young people. In addition, there is information on weapons, crime, racism and extremism that would be considered inappropriate and restricted elsewhere.

It is also known that adults who wish to abuse others may pose as a child/young person/peer to engage with them and then attempt to meet up with them. This process is known as 'grooming' and may take place over a period of months using chat rooms, social networking sites, tablets and mobile phones.

Cyberbullying:

Cyberbullying is bullying through the use of communication technology and can take many forms e.g. sending threatening or abusive text messages, e-mails or through messaging within social media websites. This bullying can be either personally or anonymously directed at individuals, making insulting comments about someone on a social networking site or blog or making/sharing derogatory or embarrassing videos of someone via mobile phone or e- mail.

Sexting:

This involves users sending sexually explicit texts in the form of images or video to other children or adults. These images are often then distributed further without permission, which poses a significant safeguarding risk and places them at risk of further harm.

Why internet and digital communications are important:

Teaching and learning:

- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.
- We believe that the use of Internet and is a necessary tool for staff and pupils. The children learn how to use the internet to find, search, exchange and share information.
- The school Internet access is provided by Nottinghamshire County Council and includes filtering set an appropriate level for pupils at our school. The level of filtering restricts access to inappropriate content but is not so restrictive that children and adults cannot access important tools for teaching and learning in school.
- Pupils will be taught what Internet use is acceptable and what is not and given clear guidelines for Internet use.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- Pupils will be shown how to publish and present information appropriately to a wider audience.

Pupils will be taught how to evaluate Internet content:

- The school will seek to ensure that the use of Internet derived materials by staff and by pupils complies with copyright law.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Pupils will be taught how to report unpleasant Internet content.

In addition to accessing the internet in organisation settings, children, young people and vulnerable adults may access the internet and/or use other digital technologies in their own time at other locations. This is when they will be at greater risk if they have not been taught about how to use them safely and what the dangers are.

Managing Internet Access & Roles and Responsibilities:

Governors

Governors are responsible for the approval of the E-safety policy and for reviewing the effectiveness of the policy by reviewing E-safety incidents and monitoring reports. E-safety falls within the remit of the governor responsible for Safeguarding. The role of the E-safety Governor will include:

- Ensure an E-safety policy is in place, reviewed every 3 years (or earlier if required) and is available to all stakeholders
- Ensure that there is an E-safety coordinator who has been trained to a higher level of knowledge which is relevant to the school, up to date and progressive
- Ensure that procedures for the safe use of ICT and the Internet are in place and adhered to
- Hold the Headteacher and staff accountable for E-safety.

Headteacher and SMT

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 Data Protection Officer (DPO). Any complaint about staff misuse must be referred to the DPO at the school or, in the case of a serious complaint or allegation which breaches safeguarding procedures, to the Headteacher.

- Ensure access to induction and training in E-safety practices for all users.
- Ensure appropriate action is taken in all cases of misuse.
- Ensure that Internet filtering methods are appropriate, effective and reasonable.
- Ensure that staff or external providers who operate monitoring procedures be supervised by a named member of SMT.
- Ensure that pupil or staff personal data as recorded within school management system sent over the Internet is secured.
- Work in partnership with the DfE, Local Authority and the Internet Service Provider, Computing Leader and FrogboxIT to ensure systems to protect students are reviewed and improved.
- Ensure the school ICT system is reviewed regularly with regard to security and that virus protection is installed and updated regularly in partnership with FrogboxIT

Computing coordinator:

The Computing Coordinator will undertake relevant training to ensure the school is aware of the key messages in relation to keeping children safe online and ways to tackle child exploitation. This will also be complemented by regular training in line with the PREVENT duty to protect children from the risks of radicalisation and extremism. Other duties include:

- Leading E-safety staff meetings and workshops for parents.
- Works in partnership with the DfE, Local Authority and the Internet Service Provider, to ensure systems to protect students are reviewed and improved.
- Ensure the school ICT system is reviewed regularly with regard to security and that virus protection is installed and updated regularly.
- Receives reports of E-safety incidents and creates a log of incidents to inform future E-safety developments.

Network Management:

FrogboxIt is responsible for ensuring:

- That the schools technical infrastructure is secure and is not open to misuse or malicious attack.
- That the school meets required E-safety technical requirements and any 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 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.
- That the use of the network / internet / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher; DPO for investigation / action / sanction
- That monitoring software / systems are implemented and updated as agreed in school policies.
- Updating of the relevant virus protection.
- Discussing security strategies with the Local Authority, Internet Service Provider and other link Governor.

E-mail:

- Staff may only use approved e-mail accounts which will be checked to ensure they offer added protection of information sharing.
- Pupils may have access to a class email address for teaching purposes
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone they meet online.
- Staff to pupil/parent email communication must only take place via a school email address and will be monitored.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- The forwarding of chain letters is not permitted.
- Staff to staff e-mails concerning children should use initials as identification, not names.

Publishing pupil's images and work

Images or videos of children are considered to be forms of personal information:

Pupils' full names will be avoided on the school website, particularly in association with photographs. If a photo is used in any context, the child's full name should not be.

Written permission from parents or carers will be obtained before photographs or videos of pupils are used in school or published on the school website. This will be obtained when the child joins the school to cover all uses, although a parent may withdraw their permission in writing at any time.

SD cards, memory sticks and CDs are a temporary means of storage for images. Once they have been used or uploaded to a secure location (e.g. the school network) they should be removed from the temporary storage device.

Images obtained via a third party are subject to copyright and either verbal or written permission should be obtained before they are used.

During performances in school, parents and guardians will be reminded that photographs and videos taken must be retained only for their own personal use and not posted online without the express permission of all of the parents or guardians of the children shown.

Social networking and personal details:

- The school will limit access to social networking sites, and consider how to educate pupils in their safe use
  e.g. use of passwords.

- Pupils will be advised never to give out personal details of any kind which may identify them or their location.

- Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils.

- Pupils will be advised to use nicknames and avatars when using social networking sites.

Managing filtering and access to inappropriate content:

- The school will work in partnership with Nottinghamshire County Council to ensure systems to protect pupils are reviewed and improved in line with the most recent guidance.
- If staff or pupils come across unsuitable on-line materials, the site must be reported to a member of the Senior Management Team.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- Class Teachers will be responsible for overseeing the content that children access, particularly in places outside of the classroom (corridor computers or use of portable technologies) or at times outside of lessons (break times or after school clubs).

Managing emerging technologies:

- Emerging technologies will be examined for educational benefit and the potential risks assessed before use in school is allowed.
- Children will not use personal mobile phones and associated cameras during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.
- Staff will use a school phone where contact with pupils is required.

Protecting personal data:

The school is responsible for reviewing and managing the security of the computers and Internet networks as a whole and takes the protection of school data and personal protection of our school community very seriously. This means protecting the school network, as far as is practicably possible, against viruses, hackers and other external security threats. FrogboxIT will review the security of the school information systems and users regularly and virus protection software will be updated regularly. Some safeguards that the school takes to secure our computer systems are:

- Ensuring that all personal data sent over the Internet or taken off site is encrypted
- Making sure that unapproved software is not downloaded to any school computers. Alerts will be set up to warn users of this
- Files held on the school network will be regularly checked for viruses
- The use of user logins and passwords to access the school network will be enforced
- Portable media containing school data or programmes will not be taken off-site without specific permission from the Headteacher or DPO.

With effect from 25th May 2018, the data protection arrangements for the UK change following the European Union General Data Protection Regulation (GDPR) announced in 2016. For more information on data protection in school please refer to our **data protection policy**.

Data Storage and Transport:

All personal information must be kept secure. We employ a combination of technical and procedural solutions to maximise the security of personal data (including photographs) of children or adults:

- All staff laptops will be password protected and staff will be encouraged to change these regularly.
- Transporting personal information off site should be avoided unless necessary.
- If personal data is required to be taken off site, it should either be stored on a password protected laptop or an encrypted memory stick and be deleted when no longer needed.
- An adult should take all necessary precautions when using a school laptop at home to make sure that no material is accessed which could contravene any elements of this policy (e.g. this has implications for uploading personal photographs, personal use of the internet, allowing other people to use the machine, etc.)

Policy Decisions Authorising

Internet access:

1. All staff must read and sign the '**Staff Acceptable Use Agreement** ' before using any school ICT resource or personal device in school.
2. The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.
3. Any child who is deemed a high risk when using the Internet or any ICT equipment / resource will have restricted access in school and in this exceptional circumstance, parents will be consulted on the management of Computing curriculum provision offered to their child.
4. Parents will be asked to sign and return a consent form.
5. Any person not directly employed by the school will be reminded of the school's 'acceptable use of school ICT resources' before being allowed to access the Internet from the school site. Use of ICT resources will be monitored closely.

Assessing risks:

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor NCC can accept liability for the material accessed, or any consequences of Internet access.
- The school will audit ICT use to establish if the E-safety policy is adequate and that the implementation of the E-safety policy is appropriate and effective.

Handling E-safety complaints:

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the Headteacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the complaints procedure.
- Pupils and parents will be informed of consequences for pupils misusing the Internet.

Communications Policy

Introducing the E-safety policy to pupils:

- Appropriate elements of the E-safety policy will be shared with pupils.
- E-safety posters (**Think then click or tap**) will be posted nearby to where computers or mobile devices may be used.
- Pupils will be informed that network and Internet use will be monitored.
- Curriculum opportunities to gain awareness of E-safety issues and how best to deal with them will be provided for pupils.

Staff and the E-safety policy:

- All staff will be directed to read the school's E-safety Policy and its importance explained.
- All members of staff will be asked to sign the **Acceptable Use Agreement**.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff that manage filtering systems or monitor ICT use will be supervised by senior management and have clear procedures for reporting issues.

Enlisting parents' support:

- Parents' and guardians' attention will be drawn to the School E-safety Policy in newsletters, the school brochure and will be made available on the school website
- Parents and carers will from time to time be provided with additional information on E-safety – such as parent workshops.
- The school will ask all new parents to sign the parent /pupil agreement when they register their child with the school.
- In instances where the school has concerns about a child's home access to computers or online technologies including incidences of: Cyber-Bullying, meeting strangers, accessing inappropriate content such as video games above the recommended age certificate, the Child Protection Policy will be referred to and concerns dealt with in accordance with its procedures.

Acceptable Use Agreement

Introduction

This Policy has been written by the school, involving all stakeholders and builds on best practice and government guidance. It relates to the latest version of DfE statutory guidance: **'Keeping Children Safe in Education'**.

This agreement should also be read in conjunction with the most recent version of the **Staff Handbook,** which sets out the **Staff Code of Conduct**, use of electronic devices and social networking sites, safeguarding children and our expectations for upholding the highest standards of professional conduct both in and outside of the school workplace.

The aims of this policy are:

- To encourage safe use of the Internet by both children and adults working within our school.
- To encourage the development of skills to access, analyse and evaluate resources from the Internet.
- To use these resources to support teaching and learning across the curriculum.
- To ensure their supervised and appropriate use.

Guidelines:

As access can lead to any publicly available resources on the Internet, a filtered/screened service will be used in school to block access to the majority of unsuitable sites. This will ensure access to unsuitable material is minimised.

Children will be shown how to find and access information on suitable web search engines, such as 'Google'.

When a child enters the school, parents and children will be asked to consent to 'an acceptable use of the internet' contract which will be kept on file for reference.

All staff members will be aware of their responsibilities towards pupils, checking sites they recommend are suitable, ensuring that access is supervised and that appropriate rules are being followed.

In so far as possible, screens should always be facing the teacher. Where this is not the case the teacher must walk regularly around the group to supervise sites being accessed. Children should be aware of the problems associated with Internet access and should be encouraged as a class to develop their own Internet rules before the class uses the Internet. They should know that by using 'history' and 'cookies', the teacher can review what has been accessed.

If possible, a written record is to be kept of any undesirable material that is accessed inadvertently. Contact with the ISP will be made if necessary to adjust filtering settings.

Emails:

Class based addresses are available for the children to use and may be available to each class teacher when required. No e-mail should be sent from the school without a member of staff approving it. Pupils should be identified by the name in the subject area of the e-mail, not in the address. Teachers are responsible for the e-mail that is received by their class.

The use of Chat rooms, or sharing sites such as Seesaw, to support teaching and learning will be closely monitored to protect against incidents of cyberbullying. Children will be taught, as stated in the E-safety Policy, about keeping themselves safe when using the Internet.

Virus Protection:

Virus protection is installed and kept up to date in school (ESET Endpoint Anti-Virus). Computer users, especially Internet users, should be aware of the dangers of virus corruption from Internet downloads or attachments to e-mails. Daily virus updates to the school network will be used to help prevent damage to files and systems.

Internet and System Monitoring:

All Internet activity is monitored by the school system and checked by FrogboxIT. It is the responsibility of the ICT co-ordinator to review this activity periodically. It is the duty of the ICT co-ordinator to report any transgressions of the school's Internet policy and/or use of obscene, racist or threatening language detected by the system to the Headteacher. Occasionally, it may be necessary for the ICT co-ordinator to investigate attempted access to blocked sites, and in order to do this, the ICT co-ordinator will need to set his/her Internet access rights to "Unrestricted". Whenever this happens, this should be recorded in the ICT violations register, and the Headteacher notified.

Any serious transgressions of the school's E-safety Policy will be recorded and dealt in accordance with the school Behaviour Policy or for adults, the relevant Safeguarding Policy, or Staff Code of Conduct.

Internet Publishing Statement:

The school wishes our website to reflect the range of activities and educational opportunities on offer, however, we recognise the potential for abuse that material published on the Internet may attract, no matter how small this risk may be. Therefore, when considering material for publication, the following conditions should be adhered to:

- No photograph or video recording may be published without the written consent of the parents/legal guardian of the child concerned, and the child's own verbal consent.

- Surnames of children should not be published, especially in conjunction with photographic or video material;

- No link should be made between an individual and any home address (including simply street names);
- Where the person publishing material suspects that there may be child protection issues at stake then serious consideration must be taken as to whether that material may be published or not. In the case of a simple piece of artwork or writing, this may well be fine, but images of that child should not be published. If in any doubt at all, refer to the person responsible for child protection.

Acceptable Use Agreement

Staff and Volunteers must abide by the following code of conduct:

- This covers use of digital technologies in the organisation i.e. e-mail, internet, intranet and network resources, learning platforms, software, mobile technologies, equipment and systems.
- I will only use the organisation's digital technology resources and systems for professional purposes or for uses deemed reasonable by the Head Teacher.
- I will only use secure e-mail system(s) for any organisation's business (web mail accounts are not secure e- mail system(s)).
- I will not browse, download or send material that could be considered offensive to colleagues and any other individuals.
- I will report any accidental access, receipt of inappropriate materials or filtering breaches to the manager.
- I will not allow unauthorised individuals to access e-mail / internet / intranet /networks or systems.
- I will ensure that all my login credentials (including passwords) are not shared with any other individuals, displayed or used by any individual than myself.
- I will not download any software or resources from the internet that can compromise the network or are not adequately licensed.
- I will follow the DSCF 2009 'Guidance for Safer Working Practice for Adults who work with Children and Young People' (http://www.timeplan.com/uploads/documents/Downloads/Safer-WorkingPractices.pdf
- I will ensure that my personal e-mail accounts, mobile/home telephone numbers are not shared with children, young people or families.
- I will not allow children and young people to add me as a friend to their social networking site nor will I add them as friends to my social networking site.
- I will ensure that any private social networking sites / blogs etc. that I create or actively contribute to are not confused with my professional role.
- I will ensure that the reputation of the school is not brought into question, following any messages, blogs or posts I may make online.
- I understand that all internet and network usage can be logged and this information could be made available to my manager on request.

- I will not connect a computer, laptop or other device to the network/internet that has not been approved by the organisation and meets its minimum security specification.

- I will not use personal digital cameras or camera phones for transferring images of children and young people or staff without permission.

- I will not engage in any online activity that may compromise my professional responsibilities.

- I understand that the Data Protection Act requires that any information seen by me with regard to staff or children and young people, held within any organisation system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.

- I will at all times behave responsibly and professionally in the digital world and will not publish any work- related content on the internet without permission from the Headteacher.

- I will ensure that I am aware of digital safeguarding issues so that they are appropriately embedded in my practice.

- I understand that failure to comply with this Acceptable Use Agreement (AUA) could lead to disciplinary action.

User Signature:

I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the organisation's most recent Acceptable Use Agreement (AUA).

I agree to abide by the organisation's most recent Acceptable Use Agreement (AUA).

Signature …… Date ……

Full Name …… (print)

Job title ……