Ravenbank
SCHOOL

E-SAFETY POLICY

RATIFYING COMMITTEE	Educational Standards & Achievement Committee
DATE RATIFIED	October 2019
NEXT REVIEW DATE	October 2022

ACCOUNTABLE LEAD/ POLICY AUTHOR: ICT Co-ordinator

The development of this policy has involved due regard to the requirements of the Equality Act 2010.

1. Executive Summary

Online technology 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 and Twitter

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 COMPUTING, 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 Ravenbank, 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 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 should be 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, webcams, whiteboards, voting systems, digital video equipment, etc); and technologies owned by pupils and staff, but brought onto school premises (such as laptops, smart phones, tablets and other mobile devices).

2. Contents

Section	Section Title	Page Number
1	Executive Summary	2
2	Contents	3
3	Introduction 3.1) Rationale 3.2) Scope 3.3) Principles	4
4	Policy Standards	5
5	Conditions of Use	11
6	Investigations of Violations and Corrective Action	12
7	Notification and Acceptance	12
8	Definitions	12
9	Duties	12
10	Development and Consultation and Communication with Stakeholders	13
11	Monitoring Compliance with and the Effectiveness of eSafety Policy	13
12	Supporting Documentation	13
13	Glossary of Terms	13

3 . Introduction
3.1 Rationale:

1.1 The purpose of this policy is to define acceptable use of the computing facilities of the School in conjunction with its established culture of ethical and lawful behaviour, openness, trust and integrity.

1.2 These facilities are provided to support the vision, objectives and services of the School and must be used and managed appropriately to assure the confidentiality, integrity and availability of the information for which we are responsible.

3.2 Scope:
This policy applies to all members of the school community (including staff, pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school digital technology systems, both in and out of the school
The policy has specific implications for:

- The Full Governing Body (FGB).
- The ESA Committee.
- The Head Teacher.
- The e-Safety Co-ordinator.
- Child Protection Co-ordinator.
- Computing Co-ordinator.
- Senior Teachers

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of 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 online-bullying or other Online 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 Online Safety behaviour that take place out of school.

All employees, contractors, 3rd party users, shared service users or anyone undertaking work on behalf of the School or accessing School/Warrington Borough Council (WBC) Information and Communication systems must adhere to this policy. This policy applies to all information assets owned or leased by the School, or to devices that connect to the School network or any WBC networks and services.

3.3 Principles:
The purpose of this policy is to outline standards which act as safeguards for users to enable them to safely control their ICT usage.

The objectives of the policy are to describe the standards expected in relation to:

1. Teaching and Learning associated with the use of technology.
2. Managing ICT Access including e-mail, the school web-site, social networking, filtering, new technologies and protecting personal data.

3. The handling of e-safety complaints.
4. Community use of the Internet.
5. Communication of eSafety.

The policy is based on the necessity for effective practice at a number of levels including:

- Responsible ICT use by all staff and students; encouraged by education and made explicit through published policies.
- Sound implementation of this policy in both administration and curriculum including secure school network design and use.
- Safe and secure broadband from Warrington including the effective management of filtering.
- National Education Network standards and specifications.

Ravenbank School will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor Warrington Borough Council can accept liability for the material accessed, or any consequences of internet access.

The outcomes of the defined standards of this policy will be:

A school where everyone understands eSafety.

4. The policy standards

The standards for e-safety are:

a) Teaching and learning:

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned online safety curriculum should be provided as part of Computing / PHSE / other lessons and should be regularly revisited
- Key online safety messages should be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities
- Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making
- Pupils should be helped to understand the need for the Pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school.

- Staff should act as good role models in their use of digital technologies, the internet and mobile devices
- In lessons where internet use is pre-planned, it is best practice that 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.

b) Parents / Carers

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and carers through:

- Letters, newsletters, web site
- High profile events / campaigns e.g. Safer Internet Day
- Reference to the relevant web sites / publications e.g.

www.swgfl.org.uk
www.saferinternet.org.uk
http://www.childnet.com/parents-and-carers

c) The Wider Community

The school will provide opportunities for local community groups / members of the community to gain from the school's online safety knowledge and experience. This may be offered through the following:

- Online safety messages targeted towards grandparents and other relatives as well as parents.
- The school website will provide online safety information for the wider community
- Supporting community groups e.g. Early Years Settings, Childminders, youth / sports / voluntary groups to enhance their Online Safety provision

d) Staff / Volunteers

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- It is expected that some staff will identify online safety as a training need within the performance management process.
- The ICT coordinator (or other nominated person) will receive regular updates through attendance at external training events (eg from SWGfL / LA / other relevant organisations) and by reviewing guidance documents released by relevant organisations.
- This Online Safety Policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.
- The ICT coordinator (or other nominated person) will provide advice / guidance / training to individuals as required.

e) Managing Internet Access:

i) Information System Security

A. School ICT systems capacity and security will be reviewed regularly, every half term by ESI Tech.
B. Virus protection will be updated regularly, every half term by ESI Tech. Security strategies will be discussed with Warrington.

ii) E-mail

A. Pupils may only use approved e-mail accounts on the school system.

B. Pupils must immediately tell a teacher if they receive offensive e-mail.

C. Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.

D. E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.

iii) Published Content and the School Web Site:

A. The contact details on the school website should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.

B. The School Website Manager will take overall editorial responsibility and ensure that content is accurate and appropriate. This to be supported by all staff members and issues reported to Headteacher or Website Manager as early as possible.

C. Parents and carers sign an agreement so that children's photographs and work can be shared online, (e.g through the website, Class Dojo, Ravenbank School's Twitter account and in online newspaper articles).

D. Social networking sites are blocked.

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

iv) Managing Filtering:

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities:

a. School technical systems will be managed in ways that ensure that the school meets recommended technical requirements
b. There will be regular reviews and audits of the safety and security of school technical systems
c. Servers, wireless systems and cabling must be securely located and physical access restricted
d. All users will have clearly defined access rights to school technical systems and devices.
e. The "administrator" passwords for the school ICT systems, used by the Network Manager must also be available to the Headteacher or other nominated senior leader and kept in a secure place
f. Network Manager is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
g. Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes

B. Internet filtering / monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet. N.b. additional duties for schools under the Counter Terrorism and Securities Act 2015 which requires schools to ensure that children are safe from terrorist and extremist material on the internet.

C. School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.

D. An appropriate system is in place for users to report any actual / potential technical incident / security breach to the relevant person, as agreed.

E. Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.

F. An agreed policy is in place for the provision of temporary access of “guests” (eg trainee teachers, supply teachers, visitors) onto the school systems. An agreed policy is in place regarding the use of removable media (eg memory sticks / CDs / DVDs) by users on school devices. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

i) Mobile technology

ii) Mobile technology devices may be school owned/provided or personally owned and might include: smartphone, tablet, notebook / laptop or other technology that usually has the capability of utilising the school’s wireless network. The device then has access to the wider internet which may include the school’s learning platform and other cloud based services such as email and data storage.

iii) All users should understand that the primary purpose of the use mobile / personal devices in a school context is educational. The mobile technologies policy should be consistent with and inter-related to other relevant school polices including but not limited to the Safeguarding Policy, Behaviour Policy, Bullying Policy, Acceptable Use Policy, and policies around theft or malicious damage. Teaching about the safe and appropriate use of mobile technologies should be an integral part of the school’s Online Safety education programme.

iv) Managing Emergent Technologies:

A. Emerging Technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

B. Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.

v) Protecting Personal Data:

Personal data will be recorded, processed, transferred and made available according to the current data protection legislation. The school must ensure that:

- It has a Data Protection Policy.
- It has paid the appropriate fee to the Information Commissioner’s Office (ICO).
- It has appointed a Data Protection Officer (DPO).
- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Data held must be accurate and up to date. Inaccuracies are corrected without unnecessary delay.
- The lawful basis for processing personal data (including, where relevant, consent) has been identified and documented and details provided in a Privacy Notice.
- Where special category data is processed, a lawful basis and a separate condition for processing have been identified.
- Data Protection Impact Assessments (DPIA) are carried out.
- It has clear and understood arrangements for access to and the security, storage and transfer of personal data, including, where necessary, adequate contractual clauses or safeguards where personal data is passed to third parties e.g. cloud service providers.
- Procedures must be in place to deal with the individual rights of the data subject i.e. a Subject Access Requests to see all or a part of their personal data held by the data controller.

- There are clear and understood data retention policies and routines for the deletion and disposal of data.
- There is a policy for reporting, logging, managing and recovering from an information risk incident which recognises the requirement to report relevant data breaches to the ICO within 72 hours of the breach, where feasible.
- Consideration has been given to the protection of personal data when accessed using any remote access solutions.
- All schools must have a Freedom of Information Policy which sets out how it will deal with FOI requests.
- All staff receive data handling awareness / data protection training and are made aware of their responsibilities.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.

When personal data is stored on any portable computer system, memory stick or any other removable media:

- The data must be encrypted and password protected.
- The device must be password protected.
- The device must offer approved virus and malware checking software.
- The data must be securely deleted from the device, in line with school policy once it has been transferred or its use is complete.

vi) Authorising Internet Access:

- All staff must read, sign and adhere to the 'Acceptable ICT Usage Agreement' before using any school ICT resource.
- Access to the Internet will be by directly supervised access to specific, approved on-line materials.

f) Dealing with unsuitable / inappropriate activities

- Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other technical systems. Other activities e.g. cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities.

a) Handling e-Safety Complaints

i) Complaints of Internet misuse will be dealt with by a senior member of staff.

ii) Any complaint about staff misuse must be referred to the headteacher.

iii) Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

b) Communication:

i) Online safety rules will be posted in all all classrooms and discussed with the pupils at the start of each year.

ii) Pupils will be informed that network and internet use will be monitored.

iii) All staff will be given and asked to sign the school Acceptable Use Policy and its importance explained.

iv) Staff will be made aware that internet traffic can be monitored and traced to individual user.

v) Parents attention will be drawn to the School eSafety Policy in newsletters, the school brochure and on the school website.

5. Conditions of Use

All users of the computing facilities of the School must abide by the following standards of acceptable and ethical use and must not act in such a way which would bring the school into disrepute:

Acceptable

6. You must only use the computing facilities which you have been authorised to access;
7. You must protect the confidentiality, integrity and availability of information;
8. You must respect the privacy and personal rights of others;
9. Your use of the School computing facilities must at all times comply with the law and the copyright and intellectual property rights of others;
10. All users must comply with the Data Protection Act and ensure that any data handled or processed is accordance with the principles.
11. Where you are aware of a data breach or security incident, you must report this to ICT via the appropriate channels.
12. School Data should be securely managed when taken off the school site using encrypted memory devices or password protected files.
13. You should only use your personal hand held/external devices (mobile phones/USB devices etc) in school when permission has been gained) Employees must understand that, if they do use their own devices in school, they will follow the rules set out in this agreement, in the same way as if they were using school equipment.
14. You must keep personal phone numbers and email accounts private and not use your own mobile phones or email accounts to contact pupils;
15. You should only use a school mobile phone when on a school trip.

Non- Acceptable

- You must not use either the school facilities or any other personal computing facilities to harass, defame, libel, slander, intimidate, impersonate or otherwise abuse another person;
- You must not use the facilities for the creation, collection, storage, downloading or displaying of any offensive, obscene, indecent or menacing images, data or material;
- You must not use facilities for any kind of commercial activity personal gain or conducting political activities;
- You must not install or distribute software for which you do not have a licence or copy any School provided software
- You must not use social networking sites to publish any content which may result in actions for defamation, discrimination, breaches of copyright, data protection or

other claims for damages. This includes but is not limited to material of an illegal, sexual or offensive nature that may bring the School into disrepute;

6. Investigation of Violations and Corrective Action

Where it is believed that a user has failed to comply with this policy, the violation will be investigated and the individual may be subject to the School's disciplinary procedure. Access will be withdrawn if an employee is found to be downloading information without the appropriate licence.

Any breach found to be substantiated may be considered in line with the School's Disciplinary Procedure.

In cases of potentially criminal content, the headteacher will consider whether the police and/or the LADO should be involved, following appropriate liaison with HR.

7. Notification and Acceptance

All individuals who have been granted the right to use the the School's/Council's computing facilities understand and accept this policy and supporting documentation through the terms and conditions of their contract.

8. Definitions

a) Approved e-mail account: Outlook.

9. Duties

The Full Governing Body (FGB).
The responsibility for ensuring effective systems and processes for eSafety; that all staff are aware of, and operate within the system (policy) and are trained appropriately to deliver the required standards rests with the FGB.

The FGB has delegated specific authority for the development and monitoring of the e-Safety policy to the ESA Committee in accordance with the Scheme of Reservation and Delegation outlined in the Policy for Procedural Documents.

The ESA Committee:
The ESA Committee will develop and monitor the eSafety policy and seek assurance that the standards it outlines are being implemented and applied consistently and appropriately.

The Head Teacher:
The Head Teacher has responsibility to ensure that an eSafety policy is developed; that it is implemented effectively and that systems are in place for the effective monitoring of the standards contained within the policy.

The Head Teacher has responsibility for ensuring the preparedness of the eSafety policy for approval and ratification by the ESA Committee.

The E-safety Co-ordinator:

Aimee White

Child Protection Co-ordinator:
Lesley Sweeney
COMPUTING Co-ordinator:
Aimee White

The administration staff takes overall editorial responsibility for the school website and ensures its content is accurate and appropriate.

Senior Teacher:
Lesley Sweeney

10. Development and Consultation process

This policy has been developed in consultation with a wide range of stakeholders including: members of the ESA Committee; the Lead Governor for Policies; the Head Teacher; the Child Protection Co-ordinator and all staff.

The policy has been updated to reflect changing technologies.

11. Process for monitoring compliance and effectiveness of the eSafety Policy:

System for the Monitoring of Compliance with the eSafety Policy	
Monitoring of compliance with this policy will be undertaken by:	Headteacher/COMPUTING Coordinator
Monitoring will be performed:	Every 3 years.
Monitoring will be undertaken by means of:	Review of current technologies and
Should shortfalls be identified the following actions will be taken:	The Headteacher will consider the outcomes of the review and make recommendations for change to the ESA Committee as appropriate.
The results of monitoring will be reported to:	The ESA Committee.
Resultant actions plans will be progressed and monitored through:	The ESA Committee.

12. Supporting Documentation:

This policy has been developed through building on the Warrington eSafety Policy.
Ravenbank Acceptable Use Policies.

13. Glossary of terms

A) Published Content: Information on the internet
B) Social Networking:Facebook, Twitter etc
C) Personal Publishing: Uploading onto the internet
D) Filtering: Software that allows certain websites to be blocked for school use.

Ravenbank
SCHOOL

Staff, Governor and Visitor
Acceptable Use Agreement / Code of Conduct

ICT and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with Aimee White school E-Safety coordinator.

- I understand that my use of school) systems and devices and digital communications will be monitored
- I will not use a personal device that I have brought into school for any activity that would be inappropriate in a school setting.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.
- I will not access, copy, remove or otherwise alter any other user’s files, without permission.
- I will ensure that if I take and / or publish images of others I will only do so with their permission. I will not use my personal equipment to record these images, without permission. If images are published it will not be possible to identify by name, or other personal information, those who are featured.
- I will not publish or share any information I have obtained whilst in the school on any personal website, social networking site or through any other means, unless I have permission from the school.
- I will not, without permission, make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a school device, nor will I try to alter computer settings, unless I have permission to do so.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I have read and understand the above and agree to use the school digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.
I understand that if I fail to comply with this Acceptable Use Agreement, the school has the right to remove my access to school systems / devices

User Signature
I agree to follow this code of conduct and to support the safe use of ICT throughout the school

Signature …….………………….………… Date ……………………

Full Name ……………………………….......................................(printed)

Job title . . . .

Ravenbank
SCHOOL

Pepper Street, Lymm Cheshire WA13 0JT
Tel: 01925 753926 Fax: 01925 757473
Email: Ravenbank_Primary@warrington.gov.uk

Primary Pupil Acceptable Use KS2
Agreement / eSafety Rules

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users.

- I know that the school can monitor my use of the systems, devices and digital communications.
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password.
- I will be aware of "stranger danger", when I am communicating on-line.
- I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc)
- If I arrange to meet people off-line that I have communicated with on-line, I will do so in a public place and take an adult with me.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.
- I will not use the school systems or devices for on-line gaming, file sharing, or video broadcasting (eg YouTube), unless I have permission of a member of staff to do so.
- I will act as I expect others to act toward me:
- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.
- I will only use my own personal devices (mobile phones / USB devices etc) in school if I have permission. I understand that, if I do use my own devices in the school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any hyperlinks in emails or any attachments to emails, unless I have permission.
- I will not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings.
- I understand that I am responsible for my actions, both in and out of school

All parent/carers must read this notice and ensure they complete our School Permission Form.

Primary Pupil Acceptable Use KS1
Agreement / eSafety Rules

This is how we stay safe when we use computers:

- I will ask a teacher or suitable adult if I want to use the computers / tablets
- I will only use activities that a teacher or suitable adult has told or allowed me to use
- I will take care of the computer and other equipment
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong
- I will tell a teacher or suitable adult if I see something that upsets me on the screen
- I know that if I break the rules I might not be allowed to use a computer / tablet

Parent / Carer Acceptable Use Agreement

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies provide powerful tools, which open up new opportunities for everyone. They can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school / academy systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that parents and carers are aware of the importance of online safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

The school will try to ensure that pupils will have good access to digital technologies to enhance their learning and will, in return, expect the pupils to agree to be responsible users. A copy of the Pupil Acceptable Use Policy is attached to this permission form, so that parents / carers will be aware of the school expectations of the young people in their care.

Parents are requested to sign the permission form below to show their support of the school in this important aspect of the school's work.

Permission Form

Parent / Carers Name:

Student / Pupil Name:

As the parent / carer of the above students / pupils, I give permission for my son / daughter to have access to the internet and to ICT systems at school.

(KS2)

I know that my son / daughter has signed an Acceptable Use Agreement and has received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

(KS1)

I understand that the school has discussed the Acceptable Use Agreement with my son / daughter and that they have received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my son's / daughter's activity on the systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's online safety.