

Online Safety Policy 2022

Leader(s): Toni Homer, Chris Wallis, Dan Murphy,

Contents:

- 1) Overview
- 2) Benefits of the internet for Children and Young People
- 3) Managing Internet Use at Walkley Primary School
- 4) Sheffield RHSE Curriculum
- 5) Publishing images and work on the internet
- 6) Managing other Technologies
- 7) Assessing Risk
- 8) Handling Online Safety Complaints
- 9) Communicating the contents of this policy

Appendix 1: Indicators of Risk of Sexual Exploitation via Digital and Interactive Technology

Appendix 2 Guidance for Practitioners to Minimise the Risk of Misconduct Allegations related to Digital and Interactive Technology

Appendix 3: Steps to minimise risk

Appendix 4 Acceptable Use for Staff

Appendix 5 Acceptable Use for Juniors

Appendix 6 Acceptable Use for Infants and EYFS

Appendix 7 Acceptable Use for Parents

1 Overview

Online Safety encompasses Internet technologies and electronic communications such as mobile phones and wireless technology. It highlights the need to educate children and young people about the benefits and risks of using new technology - including computers, mobile phones and online games - and provides safeguards and awareness for users to enable them to control their online experiences.

All partner organisations of Sheffield Safeguarding Children Partnership should assess the level of risk associated with the use of digital and interactive technology by children and young people in their care. Each agency needs to take appropriate steps to safeguard children, young people and staff, according to the level of risk identified. Because of the diverse nature of the work of our partner agencies, this will vary in each organisation. This Online Safety Policy provides overarching guidance to all agencies in Sheffield to safeguard children and young people. It can be adapted and used accordingly within each setting. It should also operate in conjunction with other policies including those for Behaviour,

Bullying, Curriculum, Data Protection and Security. These policies are available on our school website.

Online Safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff, children and young people; encouraged by education and awareness raising and made explicit through published policies;
- Support and guidance for parents, giving them the knowledge and confidence to be able to supervise their child's use of digital and interactive technology;
- Sound implementation of Online Safety policy in both administration and raising awareness, including secure network design and use;
- Safe and secure broadband filtering and monitoring solutions e.g. Smoothwall where applicable, or other firewalls; Network standards and specifications.

This policy provides guidance in relation to these issues. It specifically relates to the use of computers in organisations; it does not cover the use of mobile phones by children and young people. Organisations should have separate guidance in relation to this issue.

The responsibility for Online Safety should lie with the Designated Safeguarding Lead/Officer.

2 Benefits of the Internet for Children and Young People

The purpose of Internet use in organisations is to promote the wellbeing and achievement of children and young people, to support the professional work of staff and to enhance the organisation's management information and administration systems. Internet use is an essential element in 21st century life for education, business and social interaction. It is also part of the statutory curriculum from the age of 5 years. Therefore Walkley Primary School has a duty to provide children and young people with quality Internet access and equip them with the skills to be safe whilst using digital and interactive technology.

Benefits of using the Internet include:

- Access to world-wide educational resources including museums and art galleries;
- Educational and cultural exchanges between children and young people world-wide;
- Access to experts in many fields for children and young people and staff;
- Professional development for staff through access to national developments, educational materials and effective professional practice;
- Collaboration across support services and professional associations;
- Improved access to technical support including remote management of;
- Networks and automatic system updates;
- Exchange of professional issues and administration data between local, regional and national organisations;
- Access to learning and communication wherever and whenever convenient.

Walkley Primary School's access is designed expressly for children and young people's use and includes filtering appropriate to the age of children and young people. All use by staff and children is filtered through smoothwall and reported to the headteacher and computing lead. Children and young people will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use. Internet access will be planned to enrich and

extend learning and personal development activities. Staff will guide children and young people in on-line activities that will support learning outcomes, which are planned according to their age and maturity. Children and young people will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

3. Managing Internet Use at Walkley Primary School

This section provides guidance about how to manage the use of the Internet at Walkley Primary School. Children and young people should be provided with guidance in computer rooms.

Authorised Internet Access

- The organisation will maintain a current record of all staff and children and young people who are granted Internet access.
- All staff must read and sign the 'Acceptable Use Policy' or similar before using the organisation's ICT resource.
- Parents / carers will be informed that children and young people will be provided with supervised Internet access.
- Parents / carers will be asked to sign and return a consent form for children and young people's access.

World Wide Web

- If staff or children and young people discover unsuitable sites, the URL (address), time, content must be reported to sgt@walkley.sheffield.sch.uk to be restricted and filtered
- The organisation will ensure that the use of Internet derived materials by children and young people and staff complies with copyright law.
- Children and young people should be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.

E-mail

- Children and young people may not use approved e-mail accounts on the organisation system.
- Access to external personal e-mail accounts may be blocked.
- E-mails sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on organisation headed paper.
- Children, young people and their families should only contact members of staff of organisations using enquiries@walkley.sheffield.sch.uk. This includes staff who they knew before becoming service users of the organisation. Any exceptions to this should be discussed with managers within the organisation. This is to safeguard the children, young people, their families and the member of staff from allegations of misconduct.

Social Networking

- Organisations should manage/block/filter access to social networking sites as appropriate for children and young people and staff.
- Children and young people and staff should be advised never to give out personal details of any kind which may identify them or their location.
- Children and young people and staff should be advised to consider whether the photos they upload to any social network are appropriate to be seen in a public space and to control who can access their images.

- Children and young people should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block and report unwanted communications. They should be encouraged to invite known friends only and deny access to others.
- Children, young people and their families should not contact members of staff via social networking sites. Staff should not accept them as friends on social networking sites and should be encouraged to review information posted about them on such sites.

Filtering

- The organisation will work with identified colleagues within SCC to ensure suitable filtering and monitoring systems are installed and used as effectively as possible.
- Virus protection will be installed and updated regularly.
- Security strategies should be discussed with the organisation's senior management team

Staff Devices from home

- Staff are to keep mobile phones turned off and locked away during contact with children.
- Staff who require the use of their phone to access admin rights via 2 factor authentication have it cleared with the Head Teacher.
- Mobile phones and personally-owned mobile devices brought in to school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personally-owned mobile phones or mobile devices.
- Staff may use their mobile phones in rooms where children aren't present, being aware that their conversation may be audible to others.
- Staff are to ensure any wearable technology doesn't have any camera access enabled.

Pupils Devices from Home

- Children who bring devices from home into school must have them locked into the school office. They must not be used in school time.
- If children need to phone home they will be given access to a school phone
- Mobile phones and personally-owned mobile devices brought in to school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personally-owned mobile phones or mobile devices.
- If any devices are found hidden in school then sgt@walkley.sheffield.sch.uk will be informed. The device will be confiscated and secured in the office for a parent to pick up.
- Pupils should protect their phone numbers and only share them to trusted family and friends.

Protecting Personal Data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018.

4. Sheffield RHSE Curriculum

- We will explicitly teach online safety as part of the key skill component of the computing curriculum as well as part of the Sheffield RSHE curriculum.
- **In Upper KS2 the units taught are:**
 - Os1) Control and consent
 - Os2) Protecting our identity
 - Os3) Meeting strangers online
 - Os4) Personal Information, terms and conditions
 - Os5) Analysing Digital Media Bias
 - Os7) Echo Chambers
 - Os8) Does the internet make us happy?
- **In Lower KS2 the units taught are:**
 - Os1) Online strangers
 - Os2) Sharing Online
 - Os3) Friendship Online
 - Os4) Personal Information
 - Os5) Digital Media
 - Os6) Verifying content and echo chambers
- **In KS1 the units taught are**
 - Os1) Screen time
 - Os2) Personal information
 - Os3) Online strangers
 - Os4) Fake News

5. Publishing Images and Work on the Internet

- Photographs that include children and young people will be selected carefully and will not enable individuals to be clearly identified.
- Children and young people's full names will not be used anywhere on the organisation's Web site or Blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of their children are published on the organisation's Web
- Work can only be published with the permission of the children, young people and their parents or carers.

6. Managing other Technologies

Emerging technologies will be examined for educational and developmental benefit and a risk assessment will be carried out before use in the organisation is allowed.

Children and young people should not use mobile phones or other internet enabled devices during school hours.

Staff phones should be turned off in the classroom and locked away unless exemption is granted by the Headteacher.

7. Assessing Risk

The organisation will take all reasonable precautions to prevent access to inappropriate material. However, due to the international access available via the Internet, it is not possible to guarantee that unsuitable material will never appear on an organisation's computer. Neither the organisation nor Sheffield Safeguarding Children Partnership can accept liability for the material accessed, or any consequences of Internet access.

Any child, young person or member of staff who inadvertently accesses inappropriate sites or materials should immediately report the incident to the designated Online Safety lead officer and ICT Manager in the organisation.

The organisation should audit ICT use to establish if the Online Safety policy is adequate and that the implementation of the Online Safety policy is appropriate.

8 Handling Online Safety Complaints

Complaints of Internet misuse will be dealt with by the line manager as per the organisation's code of conduct.

Any complaint about staff misuse must be referred to a manager. This may either be the complainant's line manager, or the manager of the member of staff about who the complaint is being made. Children and young people and parents / carers will be informed of the complaints procedure.

Discussions will be held with South Yorkshire Police to establish procedures for handling potentially illegal issues. They can be contacted on 0114 220 2020.

9. Communicating the Contents of this Policy

Children and Young People

Rules for Internet access will be posted in all networked rooms and classrooms.

Children and young people and staff will be informed that Internet use will be monitored.

Staff

All staff will be given a copy of this policy, its importance explained and asked to sign the acceptable use policy for staff.

Staff should be made aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

Parents / Carers

Parents / carers' attention will be drawn to this Online Safety Policy in newsletters, the organisation brochure and on the organisation's web site.

Appendix 1: Indicators of Risk of Sexual Exploitation via Digital and Interactive Technology

At Risk

- Spending increasing amount of time on social networking sites and messaging apps;
- Unexplained increased mobile phone credits or new mobile phone;
- New contacts with people out of city;
- Spending increasing amounts of time with on line friends and less time with friends from school or neighbourhood;
- Going on line during the night;
- Being secretive. Using mobile phone for accessing social networks;
- Unwilling to share /show on line contacts;
- Concern that a young person's online friendship has developed into an off line relationship;
- Concern that inappropriate images of a young person are being circulated via the internet.
- Arranging to meet people they have met on line;
- Concern that a young person is having an online relationship;
- Concern that a young person is being coerced to provide images or to perform sexual acts via webcam;
- Sharing of inappropriate images amongst friends.
- Concerned that a young person is being bribed by someone for their inappropriate on line activity;
- Concern that a young person is selling images via the internet for money;
- Concern that a young person is being drawn into providing increasingly provocative/sexualised images in exchange for payment or from fear of activity being revealed to significant adults;
- Negotiating a price for sexual activity/images;
- Concern that a young person is selling sexual services via the internet.

Appendix 2: Guidance for Practitioners to Minimise the Risk of Misconduct Allegations related to Digital and Interactive Technology

All agencies will have their own professional codes of conduct, which this guidance does not intend to replace. It is guidance that relates specifically to helping professionals put safeguards in place to minimise the risk of any allegations of professional misconduct related to the use of digital technology and social media (e.g. Social networks such as Facebook, Twitter, LinkedIn, online gaming, etc.)

This guidance relates to all children up to the age of 18, whether or not they, or their families, are current or former pupils, students/service users. It is appreciated that you may have personal friends or the children of friends who are under the age of 18. But at all times you should ensure that you treat all those under the age of 18 with the respect they deserve, whoever the child or young person is.

You should always be mindful not to put yourself in a situation that may compromise you or be misinterpreted either by the child or young person, their friend, parent or carer, or any other person. This includes both personal and professional situations. It should be remembered that careless and inappropriate action in a personal setting, whether intended or not, could have significant implications for your professional life.

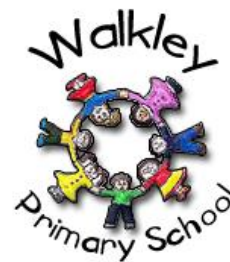
There are few professionals who have allegations of professional misconduct related to digital technology or social media made against them. However, the impact of either an allegation or cyberbullying can be significant, both personally and professionally. Taking a few steps to be pro-active in minimising any risk to yourself, whilst you may think it unnecessary, is worth taking to avoid future complications.

Remember: as a professional working with children and young people, or their families, you may be vulnerable to have an allegation made against you or being the victim of cyberbullying. Sometimes this is a result of communication or a situation being misconstrued. Other times this may be an act of revenge taken against you for an incident that has resulted through your professional practice. It may also be that someone, through having complex needs of their own, may develop an unhealthy interest in you as a person. Therefore the following steps are recommended to all professionals, and trainees who are or will be working with children, young people or their families:

Steps to Minimise Professional Risk

1. You should fully appreciate that the onus is upon you and not the child or young person to distance yourself from any potentially inappropriate situation;
2. Regularly review all content about yourself on social networking sites, such as Facebook, Twitter etc. Particularly consider removing any personal information or photographs which could be manipulated and used against you;
3. Regularly review your privacy settings on all social networking accounts;
4. Do not give personal information such as email addresses or mobile telephone numbers to anyone who is, or has been, a pupil, student/service user or is a member of their family;
5. If you wish to keep in contact with any child or young person under the age of 18, or their family, who has been a user of your service, ensure that you only use work emails or telephone numbers to communicate with them and that your Manager is aware of the contact;
6. If there is any incident, related to this guidance, which involves a child, young person or their family, that causes you concern, report it immediately to your Line manager. Document it as soon as possible, according to your workplace procedures;
7. Ensure you adhere rigidly to the Online Safety policy and Staff Acceptable Use Policy of your workplace. If you breach any part of the AUP, report it immediately as per your workplace procedures;
8. Do not access any illegal or inappropriate websites on your personal computer/laptop or mobile phone. This includes illegal or inappropriate images of children, certain other types of pornography or extremist websites. It is illegal to access or download material that promotes or depicts criminal behaviour;
9. Be very careful when liaising with others online (for example in social networks or using social media). Remember these are not private areas even though you may have privacy settings applied so likes, comments or complaints may be seen by others. Avoid inappropriate communication with individuals under 18, or with who you may be in a position of trust;
10. Use your common sense and professional judgement and expertise at all times to avoid circumstances which are, or could be, perceived to be of an inappropriate nature or which could bring your organisation into disrepute. This relates particularly to social networking sites, social media and mobile phone technology;
11. Remember, digital technology and social media may be the virtual world, but it has an impact on our real world online actions can have offline consequences.

Staff ICT Acceptable Use Policy



As a professional organisation with responsibility for children's safeguarding it is important that all staff take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft. All members of staff have a responsibility to use the school's computer system in a professional, lawful, and ethical manner. To ensure that members of staff are fully aware of their professional responsibilities when using Information Communication Technology and the school systems, they are asked to read and sign this Acceptable Use Policy.

This is not an exhaustive list and all members of staff are reminded that ICT use should be consistent with the school ethos, other appropriate policies and the Law.

- ☐ I understand that Information Systems and ICT include networks, data and data storage, online and offline communication technologies and access devices. Examples include mobile phones, PDAs, digital cameras, email and social media sites.
- ☐ School owned information systems must be used appropriately. I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.
- ☐ I understand that any hardware and software provided by my workplace for staff use can only be used by members of staff and only for educational use. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or locking my login as appropriate.
- ☐ I will respect system security and I will not disclose any password or security information. I will use a 'strong' password (A strong password has numbers, letters and symbols, with 8 or more characters, does not contain a dictionary word and is only used on one system).
- ☐ I will not attempt to install any purchased or downloaded software, including browser toolbars, or hardware without permission from Dan Hilton, Dan Murphy or Chris Wallis.
- ☐ I will ensure that any personal data of pupils, staff or parents/carers is kept in accordance with the Data Protection Act 1988. This means that all personal data will be obtained and processed fairly and lawfully, only kept for specific purposes, held no longer than necessary and will be kept private and secure with appropriate security measures in place, whether used in the workplace, hosted online (only within countries or sites with suitable data protection controls) or accessed remotely. Any data which is being removed from the school site (such as via email or on memory sticks or CDs) will be encrypted by a method approved by the school. Any images or videos of pupils will only be used as stated in the school image use policy and will always take into account parental consent.
- ☐ I will not keep professional documents which contain school-related sensitive or personal information (including images, files, videos etc.) on any personal devices (such as laptops, digital cameras, mobile phones), unless they are secured and encrypted. Where possible I

will use the School Learning Platform to upload any work documents and files in a password protected environment. I will protect the devices in my care from unapproved access or theft.

☐ I will not store any personal information on the school computer system that is unrelated to school activities, such as personal photographs, files or financial information.

☐ I will respect copyright and intellectual property rights.

☐ I have read and understood the school e-Safety policy which covers the requirements for safe ICT use, including using appropriate devices, safe use of social media websites and the supervision of pupils within the classroom and other working spaces.

☐ I will report all incidents of concern regarding children's online safety to the Designated Child Protection Coordinator (Val Sian) and/or the e-Safety Coordinator (Chris Wallis/Dan Murphy) as soon as possible. I will report any accidental access, receipt of inappropriate materials, filtering breaches or unsuitable websites to (Chris Wallis) the e-Safety Coordinator or (Dan Hilton / Dan Murphy) the designated lead for filtering as soon as possible.

☐ I will not attempt to bypass any filtering and/or security systems put in place by the school. If I suspect a computer or system has been damaged or affected by a virus or other malware or if I have lost any school related documents or files, then I will report this to the ICT Support Provider/Team (Dan Murphy / Dan Hilton) as soon as possible.

☐ My electronic communications with pupils, parents/carers and other professionals will only take place via work approved communication channels e.g. via a school provided email address or telephone number. Any pre-existing relationships which may compromise this will be discussed with the Senior Leadership team.

☐ My use of ICT and information systems will always be compatible with my professional role, whether using school or personal systems. This includes the use of email, text, social media, social networking, gaming, web publications and any other devices or websites. My use of ICT will not interfere with my work duties and will be in accordance with the school AUP and the Law.

☐ I will not create, transmit, display, publish or forward any material that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or anything which could bring my professional role, the school, or the City Council, into disrepute.

☐ I will promote e-Safety with the pupils in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create.

☐ If I have any queries or questions regarding safe and professional practise online either in school or off site, then I will raise them with the e-Safety Coordinator or the Head Teacher.

☐ I Understand that my use of the information systems, Internet and email may be monitored and recorded to ensure policy compliance.

The School may exercise its right to monitor the use of information systems, including Internet access and the interception of e-mails in order to monitor compliance with this Acceptable Use Policy and the School's Data Security Policy. Where it believes unauthorised and/or inappropriate use of the service's information system or unacceptable or

inappropriate behaviour may be taking place, the School will invoke its disciplinary procedure. If the School suspects that the system may be being used for criminal purposes or for storing unlawful text, imagery or sound, the matter will be brought to the attention of the relevant law enforcement organisation.

I understand and agree to comply with the staff acceptable use policy

Signed _____ Date _____

Junior ICT Acceptable Use Policy



New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies 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 ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

The school will try to ensure that *pupils* will have good access to ICT to enhance their learning and will, in return, expect the *pupils* to agree to be responsible users.

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

For my own personal safety:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications.
- I will not share my username and password with anyone or 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.
- 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 understand that everyone has equal rights to use technology to support our education:

- I understand that the school ICT systems are for educational use and that I will not use the systems for personal or recreational use unless I have permission 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 understand that the school has a responsibility to keep the technology secure and safe:

- I will not use my personal devices (mobile phones / USB devices etc) in school. I understand that, if I do use my own devices in 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, nor will I 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 damage or faults involving equipment or software, however this may have happened.
- I will not open any attachments to emails, unless I know and trust the person / organisation who sent the email, due to the risk of the attachment containing viruses or other harmful programmes.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings.
- I will not try to use chat and social networking sites in school.

When using the internet for research for my school work, I understand that:

- I should 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 try to download copies (including music and videos)
- When I am using the internet to find information, I should take care to check that the information that I find is accurate, as I understand that the work of others may not be correct.

I understand that I am responsible for my actions, both in and out of school:

- I understand that the school could take action against me if I am involved in incidents or inappropriate behaviour that are included in this agreement, when I am out of school as well as in school. Examples of this are: cyberbullying, sending/receiving inappropriate images and misuse of personal information.
- I understand that if I do not follow this Acceptable Use Policy Agreement, it will lead to disciplinary action. This may include loss of access to the school network / internet, detentions, suspensions, contact with parents and in the event of illegal activities involvement of the police.

Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school ICT systems.

I have read and understand the above and agree to follow these guidelines when:

- I use the school ICT systems and equipment (both in and out of school)
- I use my own equipment in school eg mobile phones, cameras etc
- I use my own equipment out of school in a way that is related to me being a member of this school eg communicating with other members of the school e.g. through social networks, mobile phones, accessing school email, Learning Platform, website etc.

Name: _____

Class: _____

Date: _____

Infant and EYFS ICT Acceptable Use Policy



This is how we stay safe when we use computers:

I will ask *a teacher / an adult* if I want to use the computer

I will only use activities that *the teacher /an adult* has told or allowed me to use. I will take care of the computer and other equipment

I will ask for help from *the teacher / an adult* if I am not sure what to do or if I think I have done something wrong.

I will tell *the teacher / an adult* if I see something that upsets me on the screen.

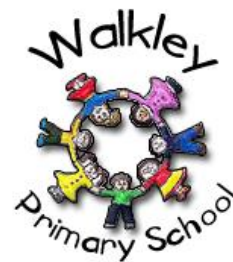
I know that if I break the rules I might not be allowed to use a computer.

Name: _____

Signed (child):.....

Signed (parent):

Parent ICT Acceptable Use Policy



New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies 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 ICT 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 e-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 ICT to enhance their learning and will, in return, expect the *pupils* to agree to be responsible users. A copy of the

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 *pupil*, I give permission for my son / daughter to have access to the internet and to ICT systems at school.

I know that my son / daughter has signed an Acceptable Use Agreement and has received, or will receive, e-safety education to help them understand the importance of safe use of ICT – 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 ICT 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 ICT 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 promote positive, safe and responsible behaviour on the internet. I will inform the school if I have concerns over my child's online Safety

Signed _____ Date: _____