Roundwood Primary School

E-Safety Policy

Name of Policy	E-Safety Policy
Date of last review	Summer 2018
Date of next review	Summer 2020*
Governing Body Committee Responsible	Resources
Member of Staff responsible	Headteacher

*Unless there is significant change in legislation

Contents

1. Introduction and Overview

Rationale

The purpose of this policy is to:

- set out the key principles expected of all members of the school community at Roundwood Primary with respect to the use of computing - based technologies.
- safeguard and protect all members of the Roundwood Primary School community.
- assist school staff working with children to work safely and responsibly with the Internet and other communication technologies and to monitor their own standards and practice.
- set clear expectations of behaviour and/or codes of practice relevant to responsible use of the Internet for educational, personal or recreational use.
- have clear structures to deal with online abuse such as cyberbullying which are cross referenced with other school policies.
- ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- minimise the risk of misplaced or malicious allegations made against adults who work with students.

The main areas of risk for our school community can be summarised as follows:

Content

- exposure to inappropriate content, including online pornography, ignoring age ratings in games (exposure to violence associated with often racist language), substance abuse.
- lifestyle websites, for example pro-anorexia/self-harm/suicide sites
- hate sites, incitement to extremism.
- content validation: how to check authenticity and accuracy of online content

Contact

- grooming
- cyber-bullying in all forms
- identity theft (including 'frape' (hacking Facebook profiles)) and sharing passwords

Conduct

- privacy issues, including disclosure of personal information
- digital footprint and online reputation
- health and well-being (amount of time spent online (Internet or gaming))
- sexting (sending and receiving of personally intimate images) also referred to as SGII (self-generated indecent images)
- copyright (little care or consideration for intellectual property and ownership – such as music and film)
  (Ref Ofsted inspection guidance Jan 2014)

Scope
This policy applies to all members of Roundwood Primary School community (including staff, pupils, volunteers, parents, carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of Roundwood Primary School.

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 cyber-bullying, or other e-safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data (see appendix for template policy). In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy (under Policies & Downloads on our website).

The school will deal with such incidents within this policy and associated Behaviour Policy and Anti-Bullying policy (under Policies & Downloads on our website) and will, where known, inform parents or carers of incidents of inappropriate e-safety behaviour that take place out of school.

Role	Key Responsibilities
Headteacher / Designated Child Protection Lead	• To take overall responsibility for e-safety provision • To take overall responsibility for data and data security (SIRO) • To ensure the school uses an approved, filtered Internet Service, which complies with current statutory requirements • To be responsible for ensuring that staff receive suitable training to carry out their e-safety roles and to train other colleagues, as relevant • To be aware of procedures to be followed in the event of a serious e-safety incident. • To ensure that there is a system in place to monitor and support staff who carry out internal e-safety procedures (e.g. Network Manager) • To ensure that an e-safety incident log is kept up to date • Liaises with the Local Authority and relevant agencies when necessary • Takes day to day responsibility for e-safety issues
Computing Subject Leader / Network Manager	• Has a leading role in establishing and reviewing the school e-safety policies and e-safety log • Promotes an awareness and commitment to e-safeguarding throughout the school community • Ensures that e-safety education is embedded across the curriculum • Liaises with school Network Manager • Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident • Facilitates training and advice for all staff • Is regularly updated in e-safety issues and legislation, and be aware of the potential for serious child protection issues to arise from: o sharing of personal data o access to illegal / inappropriate materials o inappropriate on-line contact with adults / strangers o potential or actual incidents of grooming o cyber-bullying and use of social media

	• Oversees the delivery of the e-safety element of the Computing curriculum
Governors – including the Governor responsible for Safeguarding	• Ensures that the school follows all current e-safety advice to keep the children and staff safe • Approves the E-Safety Policy and reviews the effectiveness of the policy. • Supports the school in encouraging parents and the wider community to become engaged in e-safety activities
Network Manager	• Reports any e-safety related issues that arises, to the SLT, DSPs and Computing Subject Leader • Ensures that users may only access the school's networks through an authorised and properly enforced password protection policy, in which passwords are changed termly • Ensures that provision exists for misuse detection and malicious attack e.g. keeping virus protection up to date • Ensures the security of the school ICT system • Ensures that access controls / encryption exist to protect personal and sensitive information held on the school network • Applies and regularly updates the school's policy on web filtering • Informs the LA/ web filtering provider of issues relating to the filtering applied • Monitors the school's e-safety policy and technical information in order to effectively carry out their e-safety role and to inform and update others as relevant • Regularly monitors the use of the network, data systems and email in order that any misuse or attempted misuse can be reported to the E-Safety Co-ordinator /Head teacher for investigation, action or sanction. • Ensures appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster. • Maintains up-to-date documentation of the school's e-security and technical procedures • Ensures that all data held on pupils on the school office machines have appropriate access controls in place
Teachers	• Embed e-safety issues in all aspects of the curriculum and other school activities in line with the Computing scheme of work • Supervise and guide pupils carefully when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant), using any issues that arise as teaching opportunities • Ensure that pupils are made aware of research skills and are aware of legal issues relating to electronic content such as copyright laws and creative commons licences.
All staff	• Read, understand and help promote the school's e-safety policies and guidance. • Read, understand, accept and adhere to the Staff Acceptable Use Agreement.

	• Demonstrate an awareness of e-safety issues related to the use of mobile phones, cameras and hand held devices, monitoring their use and implementing current school policies with regard to these devices. • Report any suspected misuse or problem to the Head Teacher. • Maintain an awareness of current e-safety issues and guidance e.g. through CPD. • Model safe, responsible and professional behaviours in their own use of technology. • Ensure that any digital communications with pupils should be on a professional level and only through school based systems, never through personal mechanisms, e.g. email, text, mobile phones etc.
Pupils	• Read, understand, accept and adhere to the Pupil Acceptable Use Policy. • Have an age appropriate understanding of research skills and the need to avoid plagiarism and uphold copyright regulations. • Understand the importance of reporting abuse, misuse or access to inappropriate materials. • Know what action to take if they or someone they know feels worried or vulnerable when using online technology. • Know and understand school policy on the use of mobile phones, digital cameras and hand held devices. • Know and understand school policy on the taking / use of images and on cyber-bullying. • Understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school. • Take responsibility for learning about the benefits and risks of using the Internet and other technologies safely both in school and at home. • Assist the school in the creation/ review of e-safety policies through involvement in Pupil Voice activities.
Parents/carers	• Support the school in promoting e-safety and endorse the Parents' Acceptable Use Agreement which includes the pupils' use of the Internet and the school's use of photographic and video images. • Read, understand and promote the school's Pupil Acceptable Use Agreement with their children • Access the school website in accordance with the relevant school Acceptable Use Agreement. • Consult with the school if they have any concerns about their children's use of technology.

Communication:
The policy will be communicated to staff/pupils/community in the following ways:

- Policy to be posted on the school website and stored on the shared network drive.
- Policy to be part of school induction pack for new staff.
- Policy to be part of school induction pack for governors.
- Acceptable Use Agreements discussed with pupils at the start of each year and revisited termly.

- Acceptable Use Agreements to be issued to whole school community, on entry to the school.
- Pupil and Parental Acceptable Use Agreements to be held in pupil files
- Visitor and Governor Acceptable Use Agreements to be stored centrally.
- Policy will be accepted by staff and pupils through the network on a termly basis.

Handling complaints:

- The school will take all reasonable precautions to ensure e-safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the school nor the Local Authority can accept liability for material accessed, or any consequences of Internet access.

- Staff and pupils are given information about infringements in use and possible sanctions. Sanctions available include:
    - informing parents or carers;
    - removal of Internet or computer access for a period
    - referral to LA / Police.

- The Headteacher acts as first point of contact for any complaint. Any complaint about staff misuse is referred to the Headteacher.

- Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with school / LA child protection procedures.

Review and Monitoring

The e-safety policy will be referenced from within other school policies: Child Protection Policy, Anti-Bullying Policy and Behaviour Policy.

- The school has a Network Manager and Safeguarding Governor who will be responsible for document ownership, review and updates.
- The e-safety policy will be reviewed regularly or when any significant changes occur with regard to the technologies in use within the school.
- The e-safety policy has been written and reviewed by the Computing Subject Leader, the Network manager the Headteacher and the Safeguarding Governor and is current and appropriate for its intended audience and purpose.
- There is widespread ownership of the policy and it has been agreed by the SLT and approved by Governors. All amendments to the school e-safeguarding policy will be discussed with all members of teaching staff.

2. Education and Curriculum

Pupil e-safety curriculum

This school:

- Has a clear, progressive e-safety education programme as part of the Computing curriculum / PSHE curriculum. This covers a range of skills and behaviours appropriate to their age and experience.
- Plans Internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.
- Will remind pupils about their responsibilities through an end-user Acceptable Use Policy which every pupil will accept and will be displayed throughout the school and a reminder will be displayed termly when a pupil logs on to the school network.
- Ensures staff will model safe and responsible behaviour in their own use of technology during lessons.
- Ensures that staff and pupils understand the issues around aspects of the commercial use of the Internet, as age appropriate. This may include, but is not limited to risks in pop-ups; buying on-line; on-line gaming etc.

Staff and governor training
This school:

- Ensures staff know how to send or receive sensitive and personal data and understand the requirement to encrypt data where the sensitivity requires data protection in line with the school's policies on GDPR;
- Makes regular training available to staff on e-safety issues and the school's e-safety education program.
- Provides, as part of the induction process, all new staff with information and guidance on the e-safeguarding policy and the school' computerised Acceptable Use Policies.

Parent awareness and training
This school runs a rolling programme of advice, guidance and training for parents, including:

- Introduction of the Acceptable Use Agreements to new parents, to ensure that principles of e-safe behaviour are made clear
- Information in school newsletters and on the school web site;
- Suggestions for safe Internet use at home;
- Parent workshops;
- Provision of information about national support sites for parents.

3. Expected Conduct and Incident management

Expected conduct
In this school, all users:

- are responsible for using the school ICT systems in accordance with the relevant Acceptable Use Policy which they will be expected to accept before being given access to school systems.
- need to understand the importance of misuse or access to inappropriate materials and are aware of the consequences.
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school.
- will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking and using images and on cyber-bullying.

Staff

- are responsible for reading the school's e-safety policy and using the school ICT systems accordingly, including the use of mobile phones, and hand held devices.

Pupils

- should have a good understanding of research skills and how to act responsibly and safely online.

Parents/Carers

- should provide consent for pupils to use the Internet, as well as other technologies, as part of the e-safety Acceptable Use Agreement form at time of their child's entry to the school.
- should know and understand what the 'rules of appropriate use' are and what sanctions result from misuse.

Incident Management
In this school:

- We refer to the What do we do if..? Guidance document to inform reporting pathways and appropriate responses to common e-safety issues.

- There is strict monitoring and application of the e-safety policy and a differentiated and appropriate range of sanctions, though the attitudes and behaviour of users are generally positive and there is rarely need to apply sanctions.
- All members and its wider community are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the school's escalation processes.
- Support is actively sought from other agencies as needed (e.g. the local authority and regional broadband grid, UK Safer Internet Centre helpline) in dealing with e-safety issues.
- Monitoring and reporting of e safety incidents takes place, and contribute to developments in policy and practice in e-safety within the school. The records are reviewed and audited and reported to the school's senior leaders, Governors /the LA if any incident occur.
- Parents / carers are specifically informed of e-safety incidents involving young people for whom they are responsible.
- We will contact the Police if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law.

4. Managing the ICT infrastructure

Internet access, security (virus protection) and filtering

This school:

- Has the educational filtered secure broadband connectivity;
- Uses a filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature, etc. All changes to the filtering policy is logged and only available to staff with the approved 'web filtering management' status;
- Ensures its network is healthy through use of anti-virus software;
- Uses approved software and hardware to send personal data over the Internet, ensures staff know how to encrypt files and uses secure remote access were staff need to access personal level data off-site;
- Is vigilant in its supervision of pupils' use at all times, as far as is reasonable;
- Ensures all staff and students have signed an acceptable use agreement form and understands that they must report any concerns;
- Ensures pupils only publish within an appropriate environment
- Informs all users that Internet use is monitored;
- Informs staff and students that that they must report any failure of the filtering systems directly to the e-safety co-ordinator.
- Immediately refers any material we suspect is illegal to the appropriate authorities – Police – and the LA.

Network management (user access, backup)

This school:

- Uses individual log-ins for all users;
- Stores all data in line with the requirements of GDPR regulations

To ensure the network is used safely, this school:

- Ensures staff and pupils read, discuss and accept the Acceptable User Policy.

Photographs and videos of children

- To comply with GDPR regulations, we ask for parents' permission before we photograph or make recordings of pupils.
- We follow the following rules for any external use of digital images:
    - If the pupil is named, we avoid using their photograph. If their photograph is used, we avoid naming the pupil.
- Where showcasing examples of pupils work we only use their first names, rather than their full names.
- If showcasing digital video work to an external audience, we take care to ensure that pupils aren't referred to by name on the video, and that pupils' full names aren't given in credits at the end of the film.

- Only images of pupils in suitable dress are used.

5. Data security: Management Information System access and Data transfer

The school's Data Protection Policy ensures that Roundwood Primary (the School) and its governors and employees are informed about, and comply with, their obligations under the General Data Protection Regulation (GDPR) and other data protection legislation. The School is a community school and is the Data Controller for all the Personal Data processed by the School. Everyone has rights with regard to how their personal information is handled. During the course of our activities we will process personal information about a number of different groups of people and we recognise that we need to treat it in an appropriate and lawful manner.

Strategic and operational practices

At this school:

- All members of staff take responsibility for network security and data transfer as outlined in the policy.
- Staff are clear who are the key contacts for key school information.
- Staff know how to report any incidents where data protection may have been compromised in line with data breech guidance (See GDPR policy).
- All staff are DBS checked and records are held on the Single Central Record.
- We ensure ALL the following school stakeholders accept an Acceptable Use Agreement form. We have a system so we know who has signed.
    - staff,
    - governors,
    - pupils
    - parents
    - visitors

  This makes clear staffs' responsibilities with regard to data security, passwords and access.
- We follow LA guidelines for the transfer of any data, such as MIS data or reports of children, to professionals working in the Local Authority or their partners in Children's Services / Family Services, Health, Welfare and Social Services.
- In line with GDPR regulations, material containing personal data must be encrypted in line with school policy.

Technical Solutions

- Staff have secure area(s) on the network to store sensitive documents or photographs.
- Flash drives may not be used – material containing personal data must be encrypted in line with school policy.
- We comply with the WEEE directive on equipment disposal by using an approved or recommended disposal company for disposal of equipment where any protected or restricted data has been held.
- Staff are aware through CPD what constitutes personal data and all such paper based sensitive information is shredded, using a cross cut shredder.

6. Equipment and Digital Content

Personal mobile phones and mobile devices

- Mobile phones brought into school are entirely at the staff member or visitors own risk. The School accepts no responsibility for the loss, theft or damage of any phone or hand held device brought into school.
- Pupils, below year 6, are not permitted to bring mobile phones into school. Any mobile phones brought into school by year 6 pupils must be handed into the office before the school day starts and may not be collected until after 3pm. In addition to this, pupils who bring in mobile phones **must** ensure that they are switched off when walking onto the school site and should remain so until they exit the school grounds.
- The recording, taking and sharing of images, video and audio on any mobile phone is prohibited. All mobile phone use is to be open to scrutiny and the Headteacher is able to withdraw or restrict authorisation at any time.

Digital images and video

In this school:

- We gain parental / carer permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter / son joins the school;
- We do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials / DVDs;
- Staff accept the school's Acceptable Use Policy and this includes a clause on the use of mobile phones / personal equipment for taking pictures of pupils;
- Pupils are taught that they should not post images or videos of others without their permission.

Asset disposal

Personal data held by the school will be stored in line with the school's Data Retention policy.

Details of all school-owned hardware will be recorded in a hardware inventory.

Details of all school-owned software will be recorded in a software inventory.

All redundant equipment will be disposed of through an authorised agency. This will include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data.

All redundant equipment that may have held personal data will have the storage media forensically wiped. Alternatively, if the storage media has failed, it will be physically destroyed. The school will only use authorised companies who will supply a written guarantee that this will happen.

Disposal of any equipment will conform to The Waste Electrical and Electronic Equipment Regulations 2006 and/or The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007. Further information can be found on the Environment Agency website.

7. Current Legislation and Advice

Counter-Terrorism and Security Act 2015 (Prevent), Anti-Radicalisation & Counter-Extremism Guidance
https://www.gov.uk/government/publications/preventing-extremism-in-schools-and-childrens-services

Appendices
Acceptable Use Agreement (Staff)

The computer system is owned by the school. "The computer system" means all computers and associated equipment belonging to the school, whether part of the school's integrated network or stand-alone, or taken offsite.

Professional use of the computer system is characterised by activities that provide children with appropriate learning experiences, or allow adults to enhance their own professional development.

The school recognises that technologies such as the Internet will have a profound effect on children's education and staff professional development in the coming years.

All members of staff, including students on placement, must sign a copy of this policy statement before a system login password is granted. Supply teachers will be given a supply log-in and will be required to read and sign an Acceptable Use Policy for Visitors. .

All children must be made aware through class discussion of all the important issues relating to acceptable use, especially the monitoring of Internet use.

Internet Access Policy Statement

- All Internet activity should be appropriate to staff professional activities or the children's education;
- Access is limited to the use of authorised accounts and passwords, which should not be made available to any other person;
- The Internet may be accessed by staff and children throughout their hours in school;
- Activity that threatens the integrity of the school's computer systems, or that attacks or corrupts other systems, is prohibited;
- Users are responsible for all e-mail sent and for contacts made that may result in e-mail being received. Due regard should be paid to the content. The same professional levels of language should be applied as for letters and other media. Where appropriate, emails should be sent via admin.
- Use of the school's Internet for personal financial gain (including the use of online auction sites), gambling, political purposes or advertising is excluded;
- Copyright of materials must be respected. When using downloaded materials, including free materials, the Intellectual Property rights of the originator must be respected and credited. All material saved on the school's network is the property of the school and making unauthorised copies of materials contained thereon maybe in breach of GDPR regulations, Individual Copyright or Intellectual Property Rights;
- Use of materials stored on the school's network for personal financial gain is forbidden;
- Posting anonymous messages and forwarding chain letters is forbidden;
- The use of the Internet, e-mail, or any other media to access inappropriate materials such as pornography, racist, incitement to extremism or any other offensive material is forbidden;
- All web activity is monitored, including the content of e-mail, therefore it is the responsibility of the user to ensure that they have logged off the system when they have completed their task;
- In line with the school's GDPR policy, interactive screens should not display emails and staff should log out of their emails when not at their desks;
- Children must not be given unsupervised access to the Internet. For the purposes of this policy, "supervised" means that the user is under the direct responsibility of an adult;
- The teaching of Internet safety is included in the school's Computing Scheme of Work, but all teachers within all year groups should be including Internet safety issues as part of their discussions on the responsible use of the school's computer systems, a progression grid for E-Safety is used throughout the school.

- All children must understand that if they see an unacceptable image on a computer screen, they must turn the screen off and report immediately to a member of staff.
- Refer to the 'What do we do if..?' guidance document for reporting procedures for common e-safety concerns for staff and children.

Guidance on the use of Social Networking and messaging systems

The school recognises that many staff will actively use Facebook, Twitter and other such social networking, blogging and messaging services. It is recognised that some such services may have an appropriate application in school, however, where such activities are planned a separate account should be set up for the purpose and there should be no connection made between personal and school accounts used for educational purposes. Any such accounts and activities must be approved by a member of the SLT prior to use.

Although these networks are used by staff in their own time, staff must recognise that it is not appropriate to discuss issues relating to children or other staff via these networks. Staff are encouraged to review their privacy settings regularly to make sure that their profiles and photographs are not viewable by the general public.

It is never acceptable to accept a friendship request from a child from the school as in almost all cases children of primary age using such networks will be breaching the terms and conditions of use of those networks. It is also extremely inadvisable to accept as friends ex-pupils who are still minors.

Breaches of Internet Access Policy by staff will be reported to the Head Teacher and will be dealt with according to the school's and LA's disciplinary policy, or through prosecution by law.

Internet Publishing Statement

The school wishes the school's web site to reflect the diversity of activities, individuals and education that can be found at Roundwood Primary School. From time to time the school may take photographs and videos of children for assessment purposes and for publication on the school's website etc. However, the school recognises 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 on the Internet, the following principles will be borne in mind:

- If the pupil is named, we avoid using their photograph. If their photograph is used, we avoid naming the pupil. Surnames of children must not be published, especially in conjunction with photographic or video material;
- Wherever possible children should be photographed in groups rather than as individuals;
- 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.
- All parents/carers are required to sign a document on entry indicating their consent to their child's image being taken.

Use of Computing Equipment

The installation of software or hardware unauthorised by the school, whether legitimately licensed or not is expressly forbidden.
The school reserves the right to examine or delete any files that may be held on its computer systems or to monitor any Internet sites visited.
All personal data held on the school's network is subject to the GDPR regulations and the school's Data Protection Policy.

Use of Portable Equipment

The school provides portable ICT equipment such as laptop computers, tablets, colour printers and digital cameras to enhance the children's education and to allow staff to make efficient use of such equipment to enhance their own professional activities.
Exactly the same principles of acceptable use apply as in the Acceptable Use Statement above.

- Equipment may be in the care of a specific individual, but it is expected that all staff may wish to benefit from the use of a laptop computer and access should be negotiated with the individual concerned. Any difficulties should be referred to the Computing Subject Leader or Network Manager;
- Certain equipment will remain in the care of the Computing Subject Leader or Network Manager, and may be booked out for use according to staff requirements. Once equipment has been used, it should be returned to the Network Manager's office.
- Equipment such as laptop computers may be taken offsite for use by staff in accordance with the Acceptable Use Statement and Internet Access Policy but only where express permission has been granted, ensuring that the equipment is fully insured from the moment it leaves the school premises. Note: our school insurance policy provides cover for equipment taken offsite, provided it is looked after with due care, i.e. not left in view on a car seat etc;
- Any costs generated by the user at home, such as phone bills, internet connection, printer cartridges etc. are the responsibility of the user;
- Where a member of staff is likely to be away from school through illness, professional development (such as secondment etc.) or maternity leave, arrangements must be made for any portable equipment in their care to be returned to school. In the event of illness, it is up to the school to collect the equipment if the individual is unable to return it;
- If an individual leaves the employment of the school, all equipment must be returned;
- The use of USB drives, or portable hard drives is not permitted.

- No other software, whether licensed or not, may be installed on laptops in the care of teachers as the school does not own or control the licences for such software;
- Data of a personal nature such as school reports, user credentials, correspondence, photographs and assessment data should not be taken home on a school laptop or other storage device, as it must be recognised that this data comes under GDPR regulations and is subject to the school's Data Protection Policy. All such files should be encrypted in line with school policy. It must not be transferred to home computers – if accessed via Portico, it must be removed from the device used to access it as soon as is practical. Staff are not permitted to use their own digital equipment such as cameras and mobile phones, unless express permission has been granted by the Headteacher, for example taking photographs during school visits.

Acceptable Use Policy, Roundwood Primary School, Harpenden, Hertfordshire
I confirm I have read and understood the school's Acceptable Use Policy for ICT.

Signed: _____

Date: _____

Name: _____

I will think before I click

I will keep my personal information private.

People I don't know are strangers.

I will be nice to people like I would on the playground.

If I get that 'uh-oh' feeling, I will stop and tell an adult I trust.

My name is: .....

My parent/carers name is:.....

Acceptable Use Agreement (Pupils KS2)
These rules will keep me safe and help me to be fair to others.

I agree to THINK about what I write or say online. I agree that what I write will be:
True.
Helpful.
Inspiring.
Necessary.
Kind.

I know that bullying can happen on the internet (cyber-cullying) just like it can in other places. I will remember to use STOP to remind me to **S**tart **T**elling **O**ther **P**eople if I am worried about cyber-bullying.

When working, playing or learning online, I promise to be **SMART**.
Stay safe: I won't give out personal information to people I don't know.
Don't **M**eet up : Meeting someone I have only been in touch with online can be dangerous. I will always check with an adult I trust.
Accepting files: Accepting emails, files or pictures from people I don't know can cause problems.
Reliable: I must check information before I believe it.
Tell Someone : I will tell an adult if someone or something makes me feel worried or uncomfortable.

- I will only use the school's computers and electronic equipment for schoolwork and homework.
- I will not use my personal email address or other personal accounts in school when doing school work.
- I will not sign up for any online services on a school device unless my teacher has asked me to as part of a school project.
- I will only open email attachments if it has been approved by a member of the school staff.
- I will only open or delete my files when told to by a member of staff .
- I will not tell anyone my passwords.
- I will not use other people's usernames or passwords.
- I will only edit or delete my own files and not look at, or change, other people's files without their permission.
- I will make sure that all online contact I make is responsible, polite and sensible. I will be kind and respectful at all times.
- I will not bring files into school without permission.
- I know that accounts on some websites and social networks, such as Facebook, are not available for children at primary school and will check with my parent/carer about the Age Restrictions on such sites before signing up.
- If I see anything that makes me feel upset or unhappy, I will turn off my screen and tell a teacher or another adult in school.
- If someone says, asks or posts something about me that makes me feel upset or unhappy then I will turn off my screen and tell a teacher or another adult in school.

- I understand that some people on the internet are not who they say they are and some people are not safe to be in contact with. I will not arrange to meet someone I only know on the internet. If someone asks to meet me, I will not reply to them and I will tell a teacher or parent/ carer immediately.

- I will not upload images, videos, sounds or words that could upset, now or in the future, any member of the school community as this could constitute cyberbullying.

- I understand that everything I do or receive online can be traced now and in the future. I know it is important to build a good online reputation.

- I understand that some personal devices are allowed in school and some are not and I will follow the rules. I will not assume that new devices can be brought into school without getting permission.

- I will not lie about my age in order to access games, apps or social networks that are for older people as this will put me at risk.

- I understand that these rules are designed to keep me safe now and in the future. If I break any of these rules, my teacher and/or Ms Webb will look into it and there may be a consequence.

Dear Parent/ Carer,

The internet, email, mobile technologies and online resources have become an important part of learning and life. We want all pupils to be safe and responsible when using any IT. It is essential that pupils are aware of online risk, know how to stay safe and know where to go to report problems.

Please read through these online safety rules with your child and talk with them to ensure they have understood their importance and what it means for them. When you have done this, we ask that you both sign the agreement below to say that you agree to follow these rules. Any concerns or further explanations can be discussed with Mr Barker or Ms Webb.

Please return the signed sections of this form which will be kept on record at the school.

Pupil Agreement

Pupil name:.....

This agreement is to keep me safe. I have discussed this agreement with my parents/ carers and understand the commitment I have made and my responsibilities.

Pupil signature: .....

Date: .....

Parent/s Carer/s agreement

Parent/s Carer/s agreement name/s: .....

I/we have discussed this agreement, which highlights the associated risks when accessing the internet, mobile and digital technologies, with our child. I /we agree to support them in following the terms of this agreement.

I/we also agree not to share school related information or images online or post material that might bring the school or any individual within it into disrepute. Rather than posting material online that could be construed as negative, we ask any parent/ carer, distressed or concerned about an aspect of school to make immediate contact with a member of staff. Negative postings about the school would impact on the reputation of the whole school community. Parents are encouraged to report breaches so that we can continue to protect the reputation of the school, staff, pupils and parents.

I/we also agree not to use personal mobile phones or devices within school as it would be a breach of the schools safeguarding policy. I /we understand that under no circumstances should images or videos be taken at any time at a school either on or off the school premises. I /we understand that when on the school premises or whilst representing the school in any other capacity, mobile phones or devices must be switched off and out of sight. I/we understand that members of staff will challenge us if we are seen to be in breech of this agreement.

I/we will support the school's e-safety policy and help prevent our child from signing up to services such as Whatsapp, Facebook, Instagram or Snapchat if they are underage (13 plus in most cases). I/ we will close online accounts if I/we find that these accounts are active for our underage child.

Parent/ carer signature:.....

Date:.....

Acceptable Use Policy, Roundwood Primary School, Harpenden, Hertfordshire
I confirm I have read and understood the school's Acceptable Use Policy for ICT.

Acceptable Use Agreement including photo/video permission (Parents)

	Permission granted Yes or No
Internet and computing: As the parent or legal guardian of the pupil(s) named below, I grant permission for the school to give my daughter / son access to: • the Internet at school • computing facilities and equipment at the school.	**Yes / No**
I accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the Internet and mobile technologies, but I understand that the school takes every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials.	**Yes / No**
I understand that the school can, if necessary, check my child's computer files and the Internet sites they visit at school and if there are concerns about my child's e-safety or e-behaviour they will contact me.	**Yes / No**
Use of digital images, photography and video: I understand the school has a clear policy on "The use of digital images and video' and I support this.	**Yes / No**
I understand that the school may use photographs or video of my child to support learning activities.	**Yes / No**
I accept that the school may use photographs / video that includes my child in publicity that reasonably promotes the work of the school, and for no other purpose, if given permission to do so.	**Yes / No**
I will not take photographs of children or staff at school events, nor will I share images online.	**Yes / No**
Social networking and media sites: I understand that the school has a clear policy on 'The use of social networking and media sites' and I support this.	**Yes / No**
I understand that the school takes any inappropriate behaviour seriously and will respond to observed or reported inappropriate or unsafe behaviour.	**Yes / No**
I will support the school by promoting safe use of the Internet, age-appropriate computer games/ social media sites and digital technology at home. I will inform the school if I have any concerns.	**Yes / No**

My daughter/son name(s): _____

Parent/Guardian signature: _____

Date: ___/___/___

Roundwood Primary's Policy on the use of digital images and video

To comply with GDPR regulations, we need your permission before we can photograph or make recordings of your daughter / son.

We follow the following rules for any external use of digital images:

- Where showcasing examples of pupils work we **only** use their **first names**, rather than their full names.

- If showcasing digital video work to an external audience, we take care to ensure that pupils aren't referred to by name on the video, and that pupils' full names aren't given in credits at the end of the film.

- Only images of pupils in suitable dress are used.

Examples of how digital photography and video may be used at school include:

• Your child being photographed (by the class teacher or teaching assistant) as part of a learning activity e.g. taking photos or a video of progress made by a nursery child, as part of the learning record, and then sharing with their parent / carer.

• Your child's image being used for presentation purposes around the school e.g. in class or wider school wall displays or PowerPoint© presentations.

• Your child's image being used in a presentation about the school and its work in order to share its good practice and celebrate its achievements, which is shown to other parents, schools or educators e.g. within a DVD or a document sharing good practice; in our school prospectus or on our school website.

In rare events, your child's picture could appear in the media if a newspaper photographer or television film crew attends an event.

• Your child's image being used to showcase their learning on the school website.

Note: If we, or you, actually wanted your child's image linked to their name we would contact you separately for permission, e.g. if your child won a national competition and wanted to be named in local or government literature.

Roundwood Primary's Policy on the use of Social Networking and Online Media

This school asks its whole community to promote the THINK approach when conducting ourselves in school or online.

THINK about what you are about to write or say, it is:
True?
Helpful?
Inspiring?
Necessary?
Kind?

If not, then stop!

When working, playing or learning online, we are SMART:

- **S**tay safe: Don't give out personal information to people you don't know.
- Don't **M**eet up : Meeting someone you have only been in touch with online can be dangerous. Always check with an adult you trust.
- **A**ccepting files: Accepting emails, files or pictures from people you don't know can cause problems.
- **R**eliable: Check information before you believe it.
- **T**ell Someone : tell an adult if someone or something makes you feel worried or uncomfortable.

As part of our anti-bullying policy, we take cyber-bullying very seriously. Cyber-bullying is when a children receives unkind messages or experiences other behaviour online that occurs **several times on purpose**.

If worried children should STOP:
Start
Telling
Other
People.

Any actions online that impact on the school and can potentially lower the school's (or someone in the school's) reputation in some way, or are deemed as being inappropriate, will be responded to.

In the event that any member of staff, student or parent/carer is found to be posting libellous or inflammatory comments on Facebook or other social network sites, they will be reported to the appropriate 'report abuse' section of the network site. (All social network sites have clear rules about the content which can be posted on the site and they provide robust mechanisms to report contact or activity which breaches this.)

It should be remembered that most social networking sites have age limits that prevent primary school aged children from having their own accounts.

In serious cases we will also consider legal options to deal with any such misuse.

The whole school community is reminded of the CEOP report abuse process:
https://www.thinkuknow.co.uk/parents/browser-safety/

What do we do if….?

An inappropriate website is accessed unintentionally in school by a teacher or child.

1. A child should switch their screen off and report to a teacher. Teachers should switch their screen off and play the situation down; don't make it into a drama.
2. Report to the Head teacher/Network Manager and decide whether to inform parents of any children who viewed the site.
3. Inform the school technicians and ensure the site is filtered.

An inappropriate website is accessed intentionally by a child.

1. Report to the Head teacher/Network Manager.
2. Refer to the acceptable use policy that was signed by the child, and apply agreed sanctions.
3. Notify the parents of the child.
4. Inform the school technicians and ensure the site is filtered if need be.

An inappropriate website is accessed intentionally by a staff member.

1. Report to the Head teacher/e- safety co-ordinator.
2. Ensure all evidence is stored and logged (check for report from Policy Central).
3. Refer to the acceptable use and staffing policy that was signed by the staff member, and apply disciplinary procedure.
4. Notify Governing Board.
5. Inform the school technicians and ensure the site is filtered if need be.
6. In an extreme case where the material is of an illegal nature, contact the local Police and follow their advice.

An adult uses School IT equipment inappropriately.

1. Ensure you have a colleague with you, do not view the misuse alone.
2. Report the misuse immediately to the Head teacher /Network Manager and ensure that there is no further access to the device. Record all actions taken.
3. If the material is offensive but not illegal, the Head teacher should then:
   - Remove the device to a secure place.
   - Instigate an audit of all ICT equipment by the school's ICT managed service providers or technical teams to ensure there is no risk of pupils accessing inappropriate materials in the school.
   - Identify the precise details of the material.
   - Take appropriate disciplinary action (undertaken by Head Teacher).
   - Inform the Governing Board of the incident.
4. In an extreme case where the material is of an illegal nature:
   - Contact the local Police and follow their advice.
   - If requested, remove the device to a secure place and document what you have done.

All of the above incidences must be reported immediately to the Head teacher and Network Manager.

A bullying incident directed at a child occurs through email or mobile phone technology, either inside or outside of school time.

1. Advise the child not to respond to the message.
2. Refer to relevant policies including e-safety, anti-bullying and apply appropriate sanctions.
3. Secure and preserve any evidence through screenshots and printouts.
4. Inform the sender's e-mail service provider if known.
5. Notify parents of all the children involved.
6. Consider delivering a parent workshop for the school community.
7. Inform the Police if necessary.
8. Inform other agencies if required (LA, Child Protection).

Malicious or threatening comments are posted on an Internet site (such as social networking) about member of the school community (including pupils and staff).

1. Inform and request the comments be removed if the site is administered externally.
2. Secure and preserve any evidence.
3. Send all the evidence to CEOP at http://www.ceop.gov.uk/contact_us.html
4. Endeavour to trace the origin and inform police as appropriate.
5. Inform LA and other agencies (Child protection, Governing Board etc).

In this scenario, the school may wish to consider delivering a parent workshop for the school community.

You are concerned that a child's safety is at risk because you suspect someone is using communication technologies (such as social networking sites or gaming) to make inappropriate contact with the child

1. Report to and discuss with the named Child Protection officer in school and contact parents.
2. Advise the child on how to terminate the communication and save all evidence.
3. Contact CEOP http://www.ceop.gov.uk/
4. Consider the involvement police and social services.
5. Inform LA and other agencies.
6. Consider delivering a parent workshop for the school community.

You are concerned that a child's safety is at risk because you suspect they are playing computer games that are inappropriate or certificated beyond the age of the the child

1. Report to and discuss with the named Child Protection officer in school and contact parents.
2. Advise the child and parents on appropriate games and content.
3. If the game is played within school environment, ensure that the technical team block access to the game.
4. Consider the involvement social services and child protection agencies.
5. Consider delivering a parent workshop for the school community.

You are aware of social network posts and pages created by parents about the school. While no inaccurate information is posted, it is inflammatory and disruptive and staff are finding it hard not to respond.

1. Contact the poster or page creator and discuss the issues in person.
2. Provide central staff training and discuss as a staff how to behave when finding such posts and appropriate responses.
3. Contact the Governing Board Friends association (PTA).
4. Consider delivering a parent workshop for the school community.

All of the above incidences must be reported immediately to the Head teacher and Network Manager.

Children should be confident in a 'no-blame culture' when it comes to reporting inappropriate incidents involving the internet or mobile technology: they must be able to do this without fear.