Version no.	Date	Next review
3.0	April 2016	April 2018
4.0	April 2018	April 2020
5.0	April 2020	May 2024

RAF BENSON COMMUNITY PRIMARY SCHOOL

POLICY DOCUMENT

E-Safety Policy

Signed: Signed on original		**Date:** April 2020	
Head Teacher			
Policy has been adopted/reviewed by Governing Body:			
Signed: Signed on original		**Date**: April 2020	
Chair of Governors			
Committee responsible for policy review	Curriculum, Performance and Standards Committee	**Linked Policies**	Computing Policy Safeguarding policy Curriculum Policy

E-SAFETY POLICY

Technology is a fundamental part of our everyday lives. It impacts upon the way we work, teach, learn and play. At RAF Benson Primary school we recognise that using technology can be exciting, innovative and fun, but that it can also expose us to risks and dangers, some of these are noted below:

- Access to illegal, harmful or inappropriate images and content;
- Access to videos and games that are unsuitable or inappropriate to age;
- Unauthorised access to personal information;
- Contact/communication with strangers;
- Inappropriate contact/communication with people who are not whom they portray to be online;
- Sharing of personal images without the knowledge or permission of an individual;
- Cyber-bullying;
- Illegal downloading of music or video files;
- Plagiarism and copyright infringement;
- An inability to evaluate the quality, accuracy and relevance of information on the Internet;
- Excessive use which impacts on social and emotional development and learning.

At RAF Benson Primary school we believe it is very important to give E-Safety a high profile and to ensure that anyone that uses any of our technology systems, remain safe and in control.

This policy applies to all members of the school community *(including staff, pupils, volunteers, parents/carers, visitors, community users)* who have access to or are users of school ICT systems, both in and out of school.

AIMS

We aim to help every pupil and adult to:

- Feel safe and confident when using e-resources;
- Know who to speak to if they feel unsafe or threatened;
- Know how to report anything that causes concern when using e-resources;
- Know the importance of keeping personal information private;
- Know what to do to make their accounts safe and secure;
- Know how to block and delete accounts, messages and people;
- Show respect and be polite when communicating with others using e-resources;
- Be aware of how to use the Internet correctly, to respect copyright and know how to verify information for accuracy;
- Ensure they only access sites appropriate for use in school and that are age and content appropriate;
- Be clear about what is acceptable and unacceptable behaviour when using e-resources.

ROLES AND RESPONSIBILITIES

All the adults involved in the life of our school; whether governors, teaching staff, support staff, technicians, have responsibilities relating to e-safety. Our pupils also have to take responsibility for times when they are using technology.

Governors
Our governors are responsible for the approval of this policy and for reviewing its effectiveness. Governors will monitor e-safety incident logs when required. They can also request information regarding web filtering.

Headteacher and Senior Leadership Team
The Headteacher is responsible for ensuring the safety, including e-safety, of the members of the school community, though the day-to-day responsibility for e-safety is delegated to the computing Co-ordinator.

The Headteacher and Senior Leadership Team are responsible for ensuring all staff and the Computing Co-ordinator receive current and appropriate e-safety training.

The Headteacher and Senior Leadership Team are to ensure they know the current procedures that need to be followed when a serious allegation has been made by a child or one that is in regards to a member of staff.

E-Safety Co-ordinator (Computing Subject leader)
Our E-Safety Co-ordinator is responsible for the day-to-day management of e-safety issues and has a leading role in establishing and reviewing the school e-safety policies/documents. The E-Safety Co-ordinator is also responsible for:

- Ensuring that of all staff are aware of procedures to be followed in the event of an e-safety incident;
- Providing training and advice to staff;
- Liaising with the Headteacher and Senior Management Team to receive reports of e-safety incidents and creating e-safety logs of incidents to inform future e-safety developments.
- Attending governor meetings as required to discuss current issues, review incident logs and web filtering;
- Seeking and receiving appropriate training and support to fulfil the role effectively;
- Blocking and unblocking Internet sites on the school web filtering system.

ICT Technician (123 ICT)
The ICT Technician is responsible for ensuring that:

- The school's ICT infrastructure is secure and not open to misuse or malicious attack;
- Users may only access the school's networks through a properly enforced password policy, in which passwords are changed regularly;
- Short comings in the infrastructure are reported to the Headteacher so that appropriate action can be taken.

Teaching and Support Staff
Teaching and support staff are responsible for ensuring that:

- They have an up to date awareness of e-safety matters and of the current school e-safety policy and practices.
- They have read, understood and signed the school's Acceptable Use Policy, *(AUP)* and that they abide by this policy;
- They report any misuse or problems to the E-Safety Co-ordinator/Headteacher for further investigation;
- Any digital communications with pupils such as e-mail should be strictly professional and only carried out using school systems;
- E-safety issues are embedded in the curriculum and other school activities;
- Pupils read, understand, sign and follow the Acceptable Use Policy and are aware of the E-safety policy;

- They are aware of e-safety issues related to the use of mobile phones, cameras and other hand held devices. That they monitor their use and implement current school policies with regard to these devices.

Designated Safeguarding Officers
The Designated Safeguarding Officers need to ensure they are fully trained in e-safety issues. They should be aware that serious child protection issues could occur due to:

- Cyber-bullying;
- Sharing of personal data;
- Inappropriate online conduct with adults/strangers;
- Potential or actual incidents of grooming.

Pupils
Pupils at RAF Benson Primary School are responsible for:

- Knowing the Acceptable Use Policy and abiding by these rules at all times;
- Understanding the importance of reporting abuse, misuse or access to inappropriate online materials;
- Knowing how to report incidents of online abuse, misuse, inappropriate content or anything that makes them feel uncomfortable or threatened whilst using e-resources;
- Knowing the school policy on mobile phones, cameras and other hand held devices and to recognise that these can be used for cyber-bullying;
- Understanding that the e-safety policy also covers their actions outside school, if related to their membership of the school.

Parents/Carers
Parents and Carers have the responsibility to:

- Ensure their children use e-resources safely and do not abuse these technologies;
- Abide by the school's policy with regards to using mobile phones, cameras and other hand held devices when attending school events or helping on school visits;
- Be aware of and agree to the school's Acceptable Use Policy.

E-SAFETY EDUCATION

At RAF Benson Primary School we encourage our pupils to use technology throughout the curriculum and recognise how most of our pupils have access to a range of technologies outside of school. The use of technology must be balanced by educating our pupils to take a responsible approach. We therefore see the education of our pupils in e-safety as an essential part of their education and of our e-safety provision. We believe that children need the help and support of the school to recognise and avoid e-safety risks. It is particularly important for helping our pupils to stay safe when out of school where technical support and filtering may not be available.

- All pupils will receive planned e-safety lessons through Rising Stars – Switched on Computing/PSHCE and other lessons. These lessons will be regularly revisited and revised to suit new technologies in and out of school.
- Key resources we will use when teaching e-safety will from CEOP's Think U Know website. http://www.thinkuknow.co.uk/teachers/resources
  (Hectors World at EYFS/KS1 and Cyber Cafe at KS2)
- E-safety messages will be reinforced through assemblies, e-safety week and through informal discussions when the opportunity arises.
- Pupils will be shown how to question the validity of the information they find online.

- Pupils will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the Internet.
- In lessons where Internet use is pre-planned, it is best practise that pupils should be guided to sites checked as suitable.
- When pupils are allowed to search the Internet freely, e.g. using search engines, staff must be vigilant in monitoring the websites the children visit.
- Parents will be invited to attend e-safety meetings where they will be able to ask questions and request help with setting up security measures on personal devices. They will also receive information via parent evenings, newsletters, and, can speak with the E-Safety Co-ordinator for advice before school each day.
- All staff will receive regular training for e-safety. New staff will receive e-safety training with the E-Safety Co-ordinator to ensure they are fully aware of and understand our school e-safety policy and the Acceptable Use Policies.
- The E-Safety Co-ordinator will attend e-safety update training as required and will report back to staff any new issues they need to be aware of.

TECHNICAL INFORMATION

RAF Benson Primary School receives a filtered broadband service provided by Schools Broadband; this service includes LightSpeed web filtering. The service is intended to stop users from accessing any material that would be regarded as inappropriate or illegal. The LightSpeed filtering service provided by Schools Broadband is designed to be flexible, so that the school can have ownership of what else needs to be filtered as technology advances. Sites can only be unblocked by Schools Broadband.

Up to date virus protection is installed on all computers and networks. This is Sophos on the curriculum network/computers and also Sophos on the Admin network/computers.

All personal data will be stored accordingly to the latest personal data legislation. Staff must use personal data on secure password protected machines, ensuring that they 'log off' at the end of any session. Any personal data that is stored on a USB device, portable hard drive, also needs to be password protected and encrypted.

ACCEPTABLE USE POLICIES

All members of our school community are responsible for using the school ICT systems in accordance with the appropriate Acceptable Use Policy, which they will be expected to sign before being given access to school systems.

Acceptable Use Policies are provided in the Appendix of this policy for:

~ Pupils (EYFS, KS1, KS2);
~ Staff and volunteers;
~Parents/Carers *(including permissions to use pupil images/work/video footage and for their child to use school ICT systems);*
~ Community users of the school's ICT systems.
Acceptable Use Policies are revisited with pupils annually as part of e-safety lessons. Pupils are expected to sign the AUP each year to acknowledge they have read it and intend to abide by it. Copies of the policies are sent for further discussion with parents and are displayed in classrooms.

Staff, volunteers and governors sign the relevant AUP when they take up a role in the school and again in the future if any significant changes are made to the policy.

Parents sign when their child enters our school. The parent's policy also includes permission for the school to use their child's image *(still or moving)*, and permission for their child to use the school ICT resources including the Internet.

Community users sign their AUP when they first request access to the schools ICT systems.

Computing Curriculum

We recognise that mobile phones, tablets, PDA's etc. can enhance learning and be powerful tools, but that it is also a form of technology that changes rapidly and will therefore need to be constantly revisited relating to e-safety issues.

Hand held devices *(mobile phones, voting systems, pda's, iPads)*
Members of staff are permitted to bring their personal mobile phones into school. They are required to use their own professional judgement as to when it is appropriate to use them and in conjunction with safeguarding policy and procedure. Broadly speaking this is:

- In the classroom/lesson/school visit only in an emergency or in extreme circumstances;
- Staff are free to use these devices in school, outside of teaching time in the staffroom and when children are not in school;
- Staff should not use personal devices to take digital images *(still or moving)* of children.

Pupils are not permitted to bring personal hand held devices into school.

If parents/carers volunteer to help in school or on a school visit they are not permitted to take any digital images *(still or moving)* on personal devices.

(A number of hand held devices are available in school and used by our pupils as and when considered appropriate by members of staff.)

E-mail
Access to e-mail is provided for all users in school through Microsoft Office 365. This system is currently managed by Turn IT on ICT Services, the School Finance and Personnel Officer and Headteacher.

- Staff and pupils have access to individual e-mail accounts to communicate within school. We also have class e-mail accounts overseen by class teachers.
- Staff and pupils should use only the school e-mail services to communicate with others when in school or when relating to school business.
- Pupils e-mail messages should not be considered private or secure.
- E-mail contact with the school by parents/carers should be made via the office.
- Teachers are discouraged from entering into one to one correspondences with parents via e-mail.
- Pupils are taught how to use e-mail, what is considered good practises and also the risks and dangers of using e-mail and how to deal with any incidents that occur.
- Users must immediately report, to their class teacher/E-Safety Co-ordinator – in accordance with the school policy, the receipt of any e-mail that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such e-mail.
- Parent/Carers e-mail addresses will be sought by letter when families join our school and are primarily used for newsletter dissemination. The school office holds them on record; these are not given out.

Use of digital still images and video
We recognise that using digital still images and video within the curriculum can enhance and enrich learning experiences. Digital still images and videos can be taken by either staff or

pupils for educational purposes, or be downloaded from the Internet to support learning in the classroom.

- When using digital still or moving images, staff should ensure pupils understand the risks associated with the taking, use, sharing, publication and distribution of images. In particular pupils need to know the risks attached to publishing their own images on the Internet e.g. social networking sites.
- Staff are allowed to take digital still and moving images to support educational aims and pupils are permitted under supervision of an adult. School policies concerning the sharing, distribution and publication of these images must be followed at all times.
- Care should be taken when taking digital still or moving images that pupils are dressed appropriately and are not participating in activities that might bring the individual or school into disrepute.
- Staff must ensure that they only publish, display still or moving images of pupils that we have received parental permission to use via signed agreement given to parents when their child joins our school. *(Lists displayed in ICT Suite and each class)*
- Pupils must not take, use, share, publish or distribute images of others without permission.
- Parents are permitted to take photographs/video of their children during school performances with a clear understanding that this is only for personal use and must not be shared publicly. In the case of video footage being recorded, names will be taken of parents/carers making a recording.

Use of Social Networking sites

The use of social networking sites is not permitted by staff or pupils during school hours or on school ICT systems.

Staff are not permitted to accept pupils past or present as friends on any social networking site and are discouraged from accepting parents as friends. They must not become involved in any discussions relating to our school that could cause offence or bring disrepute to our school.

Use of web based publication tools

Our school uses the public facing website www.raf-benson.oxon.sch.uk for sharing information with the community beyond our school. This includes from time-to-time celebrating work and achievements of our pupils. All users are required to consider the following good practise when publishing content on our website:

- Personal information should not be posted on the website.
- Only pupils first names are used on the website, and then only when necessary.
- Photographs published on the website or elsewhere that include pupils must be selected carefully and will comply with the following good practise guidance on the use of such images.
    - Pupil's full names will not be used anywhere on a website or blog and never in association with photographs.
    - Written permission from parents/carers will be obtained before photographs of pupils are published on the school website.
- Pupils work can only be published with the permission of the pupil and parents or carer.

Below is a table which gives a quick overview of how e-communication tools/devices are to be used by staff, pupils, parents and carers of our school. Any queries relating to this should be directed to the Computing coordinator.

COMMUNICATION TECHNOLOGY	STAFF & OTHER ADULTS				PUPILS			
	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with Staff permission	Not allowed
Mobile phones in school	√							√
Use of mobile phones in/during lessons				√				√
Use of mobile phones in social time	√							√
Taking of photographs on mobile phones or other personal devices				√				√
Taking photographs on school camera devices		√					√	
Use of personal e-mail addresses in school or on school network	√							√
Use of school e-mail for personal e-mail	√				√			
Use of personal e-mail for school business				√				√
Use of chat room facilities				√				√
Use of instant messaging		√						√
Use of social networking sites				√				√
Use of blogs		√					√	

Illegal or inappropriate activities and related sanctions

The school believes that the activities listed below are inappropriate in a school context **(those in bold are illegal)** and that users should not engage in these activities when using school equipment or systems (in or out of school).

Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:

- **Child sexual abuse images (illegal – The Protection of Children Act 1978).**
- **Grooming, incitement, arrangement or facilitation of sexual acts against children (illegal – Sexual Offences Act 2003).**
- **Possession of extreme pornographic images (illegal – Criminal Justice and Immigration Act 2008)**

- **Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) (illegal – Public Order Act 1986).**
- Pornography.
- Promotion of any kind of discrimination.
- Promotion of racial or religious hatred.
- Threatening behaviour, including promotion of physical violence or mental harm.
- Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute.

Additionally the following activities are also considered unacceptable on IT equipment provided by the school:

- Using school systems or equipment to run a private business.
- Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by Oxfordshire County Council and/or our school.
- Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions.
- Revealing or publicising confidential or proprietary information (e.g. financial/personal information, databases, computer/network access codes and passwords).
- Creating or propagating computer viruses or other harmful files.
- Carrying out sustained or instantaneous high volume network traffic (downloading/uploading files) that causes network congestion and hinders others in their use of the Internet.
- On-line gambling and non-educational gaming.
- Use of personal social networking sites/profiles for non-educational purposes.

All users will be made aware of what is acceptable or not acceptable by the Acceptable Use Policies. If unacceptable use is carried out the correct sanctions and reporting procedures will be in place. All staff are aware of who to speak to in the first instance. This is the computing coordinator, who will investigate the matter. If the matter is of a serious nature the either the Child Protection Officer or Headteacher will be informed, who will take the matter further.

All pupils will be made aware of the importance to report any incident to either an adult at school that they can trust or using the ‘Report Abuse’ button that is present on the school website, regarding any incidents that may occur outside school.

If an incident has occurred due to carelessness, which is more likely to be the case, this too will be investigated and suitable/correct sanctions will be implemented. The following tables indicate how different offences will be dealt will in regards to both pupils and staff. In all cases the Headteacher when notified will decide what action to take and whether the incident needs further action e.g. reporting to police, local authority.

Incidents / Pupil sanctions	Refer to class teacher	Refer to computing Co-ordinator	Refer to Headteacher	Refer to Police	Refer to technician E-Safety co, for	Inform parents or carers	Removal of Internet /network access	Warning	Further sanction i.e. exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in previous section on unsuitable/inappropriate activities).	√	√	√		√	√	√	√	√
Unauthorised use of non-educational sites during lessons.	√				√		√		
Unauthorised use of mobile phone/digital camera or other hand held device.	√		√			√			
Unauthorised use of social networking/instant messaging/chat rooms/personal e-mail.	√				√				
Unauthorised uploading or downloading of files.	√				√				
Allowing others to access school network by sharing username and passwords.	√	√	√		√		√		
Attempting to access the network or an online secure application using another pupil's account.	√	√	√		√		√		
Attempting to access or accessing the network or any online secure application using the account of a member of staff.	√	√	√				√		
Corrupting or destroying the data of other users.	√	√	√			√	√	√	
Sending an e-mail, text or instant message that is regarded as offensive, harassment or of a bullying nature.	√	√	√			√		√	
Continued infringements of the above, following previous warnings or sanctions.	√	√	√	√		√	√	√	√
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school.	√	√	√			√		√	
Using proxy sites or other means to subvert the school's filtering system.	√	√	√		√		√	√	
Accidentally accessing offensive or pornographic material and failing to report the incident.	√	√	√		√	√			
Deliberately accessing or trying to access offensive or pornographic material.	√	√	√	√	√	√	√	√	√
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act.	√	√	√		√	√	√	√	

Staff sanctions Incidents	Refer to line manager	Refer to Headteacher	Refer to Authority /HR	Refer to Police	Refer to technician or computing co, for	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in previous section on unsuitable/inappropriate activities).	√	√	√	√	√	√	√	√
Excessive or inappropriate personal use of the Internet/social networking sites/instant messaging/personal e-mail.	√	√			√	√		
Unauthorised uploading or downloading of files.	√	√			√	√		
Allowing others to access school network or online secure applications by sharing username and passwords or attempting to access or accessing the school network or online secure applications using another person's account.	√	√				√		
Careless use of personal data e.g. holding or transferring in an insecure manner.	√	√				√		
Deliberate actions to breach data protection or network security rules.	√	√			√	√	√	
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software.	√	√	√			√	√	√
Sending an e-mail, text or instant message that is regarded as offensive, harassment or of a bullying nature.	√	√	√			√	√	
Using personal e-mail/social networking/instant messaging/text messaging to carry out digital communications with pupils.	√	√	√			√		
Actions that could compromise the staff member's professional standing.	√	√				√		
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school.	√	√				√		
Using proxy sites or other means to subvert the school's filtering system.	√	√			√	√	√	
Accidentally accessing offensive or pornographic material and failing to report the incident.	√	√			√	√		
Deliberately accessing or trying to access offensive or pornographic material.	√	√	√		√	√	√	
Breaching copyright or licensing regulations.	√	√				√		
Continued infringements of the above, following previous warnings or sanctions.	√	√	√			√	√	√

Policy ownership and review

This policy has been written by the computing co-ordinator through consultation with the Headteacher and Senior Management Team. A draft of the policy has then been distributed to all staff for consultation. A final draft has then been presented to the Governors Curriculum committee for further consultation. The final policy has then been presented to the full governing body to be ratified. Parents have been notified via a newsletter that the policy is available on the school website.

ACKNOWLEDGEMENTS

Information has been used from a range of sources including the following:

Oxfordshire County Council
Herefordshire grid for learning
London grid for learning

APPENDIX

Acceptable Use Policies
Parent/Carer permission forms

E-RESOURCES ACCEPTABLE USE POLICY/AGREEMENT (Reception/KS1)

I will:


Always follow the instructions of my teacher.


Keep my personal information private.


Only use activities that an adult says are ok.


Always tell an adult if I see something that upsets me when using ICT equipment


I will take care of the ICT equipment I use.

I will not:


Send anyone a message which is not nice.


Use any other person's login for email or other e-resources.


Tell a stranger any of the following information:

- my name
- my home address
- my telephone numbers
- any other personal information about myself or any of my friends.

I know that if I break these rules I might not be allowed to use the computer or other ICT equipment.

I understand these computer rules and will do my best to follow them.

My name:		DATE
signed (child)		

E-RESOURCES ACCEPTABLE USE POLICY/AGREEMENT (KS2)

I understand that while I am a member of RAF Benson Primary School I must use technology in a responsible way.

For my own personal safety

- I understand that my use of technology (especially when I use the Internet) will, wherever possible be supervised and monitored.
- I will only access sites that are suitable for use in school. *(This also applies outside of lesson time)*
- I will keep my passwords safe and will not use anyone else's.
- I will keep my personal information safe as well as that of others.
- I will always tell a trusted adult if I ever see, hear or read anything which makes me feel uncomfortable while using the Internet, e-mail or any other online resource.
- I am aware that the information on an Internet site may not be accurate or may be biased. I will try to verify the information using other resources, if possible, before using it.
- I will check with my teacher or other staff member before sending e-mail, opening e-mail attachments or completing online questionnaires or memberships.
- I will always log out when I have finished using any ICT resources.

For the safety of others

- I will not interfere with the way others use their technology.
- I will be polite and responsible when I communicate with others.
- I will not take or share images of anyone without their permission.
- I will not use or send bad, threatening or annoying language nor any language which might cause hatred against any ethnic, religious other minority.

For the safety of the school

- I will not try to access anything that is illegal.
- I will not download anything that I do not have the right to use.
- I will respect copyright and trademarks. *I know that you cannot use words or pictures from the Internet without acknowledging who produced the information originally. I know that I must not copy text or pictures from the Internet and use it as my own work.*
- I will not use or bring personal hand held devices into school, including a mobile phone unless specific permission has been given.
- I will not deliberately bypass any systems designed to keep the school safe such as filtering of the Internet.
- I will tell a member of staff if I find damage or faults with technology, however this may have happened.
- I will not attempt to install or download programmes on any ICT devices belonging to the school.

I understand that I am responsible for my actions and the consequences. I understand that if I break these rules I might not be allowed to use the school ICT equipment and that if I make a serious breach of these rules external agencies might be involved: certain activities may be considered to be a criminal offence.

Name:		DATE:
Signed:		

E-RESOURCES ACCEPTABLE USE POLICY/AGREEMENT – Staff & Volunteers

Technology has transformed how we teach and work with young people, it has transformed the way we learn ourselves and the way our pupils learn, it has also transformed entertainment and the way we communicate. However, the use of technology can also bring risks. All users are entitled to have safe access to the Internet/e-resources at all times.

I understand that I must use school ICT systems and equipment in a responsible way, to ensure that there is not risk to my safety or to the safety and security of the ICT systems and other users. I will, where possible, educate the pupils in my care in the safe use of ICT and embed e-safety in my work with the pupils.

For my professional and personal safety

- I understand that the school will monitor my use of the ICT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of school ICT systems and equipment out of school. *(e-mail, laptops, MIS)*
- I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school in the e-safety policy.
- I will not disclose my username or password to anyone else, nor will I try to use anyone else's username and password.
- I will immediately report illegal, inappropriate or harmful material or incident I become aware of, to the appropriate person.
- I will close down browsers and log out of any e-resources/computer when I have finished.

Being professional in my communications and actions when using school ICT systems

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner. I will not use aggressive or inappropriate language and I appreciate that other may have different opinions.
- I will ensure that when I take/or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital images. I will not use my personal equipment to record these images, unless explicit permission to do so has been given. Where these images are published e.g. on the school website, I will not identify by name, or other personal information, those who are featured.
- I will not use social networking or chat rooms in school, or on school systems. I will also not accept pupils past or present as friends or contact pupils past or present on any social networking sites. I must not become involved in any online/social networking discussions relating to our school that could cause offence or bring disrepute to our school or members of our school.
- I will only communicate with pupils and parents/carers using official school systems. Any such communication will be professional in tone and manner.
- I will not use school systems or equipment for business, profit, advertising or political purposes.
- I will not engage in any online activity that may compromise my professional responsibilities.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school.

- I will only use my personal mobile/hand held devices as agreed in the e-safety policy and then in the same way as if I was using school equipment. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not use personal e-mail addresses for communicating any school business.
- I will not open any attachments to e-mails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
- 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 any of the above materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up Internet capacity and prevent other users form being able to carry out their work.
- 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, unless this is allowed in school policies.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School/LEA Personal Data Policy. Where personal data is transferred outside the secure school network, it must be encrypted.
- I understand that data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I understand that I must use personal data on secure password protected machines, ensuring that I 'log off' at the end of any session. If I store any sensitive or personal data on a USB device, portable hard drive, it must be password protected and encrypted.
- I will immediately report any damage or faults involving equipment or software, however they may have happened.

When using the Internet/e-resources/e-mail with pupils

- I will remind pupils of the rules for keeping safe when using any e-resource.
- I will vigilant in watching for accidental access to inappropriate materials and report the offending site to the E-Safety C0-ordinator.
- I will be aware of issues relating to cyber-bullying and watch for evidence of any distress caused by the use of ICT and investigate its cause.
- I will check before publishing pupils work; making sure I have parental permission.
- I will ensure pupils cannot be identified from photographs and ensure that pupils do not use any personal photographs on their personal homepage of subscribed resources.
- I will report any breaches of the school's e-safety policy to the E-Safety Co-ordinator and Headteacher.

When using the Internet in my professional capacity or for sanctioned personal use

- I will ensure that I have permission to use 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 understand that I am responsible for my actions in and out of school;

- I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment out of school and my use of personal equipment in school or in situations related to my employment by the school.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could involve a warning, a suspension, referral to Governors and/or the Local Authority and in the event of illegal activities the involvement of the police.

I have read and understand this Acceptable Use Policy Agreement and agree to abide by it and to use the school ICT systems (both in and out of school) within these guidelines.

Staff/volunteer name:	
Signed:	
Date:	

E-RESOURCES ACCEPTABLE USE AGREEMENT AND PERMISSION FORMS - Parent/carer

Technology has transformed learning, entertainment and communication for individuals and for all organisations that work with young people. However, the use of technology can also bring risks. All users are entitled to have safe access to the Internet/e-resources at all times. This Acceptable Use Policy is intended to ensure:

- That your child(ren) will be a responsible user(s) and safe while using technology (especially the Internet).
- 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 you as parents/carers are aware of the importance of e-safety and are involved in the education and guidance of your child(ren) with regard to their online behaviour.

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

Parents/carers we request you to sign the permission request below to show your support of the school in this important aspect of the school's work.

Child's name: *(please give all names of children in our school)*	
Parent's/carers name:	
Parents/carers signature:	
Date:	

Permission for my child to use the Internet and electronic communication

Please note phrases in bold with an *, it is very important that you delete as applicable.

As the parent/carer of the above pupil(s), **I do/do not*** give permission for my child(ren) to have access to the Internet and to ICT systems at school.

I know that my child(ren) 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 pupils stay safe when they use the Internet and ICT systems. I also understand that the school cannot ultimately be responsible for the nature and content of materials accessed on the Internet and using mobile technologies.

I understand that my child's(ren'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(ren) 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 (ren's) e-safety.

E-RESOURCES ACCEPTABLE USE POLICY/AGREEMENT – Community User

You have requested use of our school's ICT facilities. Before we can give you a log-in or the wi-fi connection passcode we need you to agree to this Acceptable Use Policy.

For my professional and personal safety

- I understand that he school will monitor my use of the ICT systems, email and other digital communications.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username or password.
- I will immediately report any illegal, inappropriate or harmful material or incident, of which I become aware, to a member of the school's staff.

Being professional in my communications and actions when using school ICT systems

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not use social networking or chat rooms in school, or on school systems. I must not become involved in any online/social networking discussions relating to our school that could cause offence or bring disrepute to our school or members of our school.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school.

- I will not open any attachments to e-mails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
- I will only use my personal mobile/hand held devices as agreed in the e-safety policy and then in the same way as if I was using school equipment. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- 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 any of the above materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up Internet capacity and prevent other users form being able to carry out their work.
- 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, except with the specific approval of the school.
- 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 they may have happened.

I have read and understand the above and agree to use the school ICT systems and equipment within these guidelines. I understand that failure to comply with this agreement will result in my access to the school's system being withdrawn.

Community user, Name:	
Signed:	
Date:	