Barrs Court Primary School

E-Safety Policy

(Statutory Policy Document)

Version No 1

March 2022

Date approved by Headteacher	March 2021	
Date approved by Staff	March 2021	
Committee Responsibility	**Name of Committee:**	**Date of Approval:**
	SC&S	March 2022
Date of Full Governing Body Approval (if required)	March 2022	
Policy Review Frequency	Annually	
Next Review Date	March 2023	

Barrs Court Primary School
E-safety Policy

Why is Internet Access Important?

The development and expansion of Computing, and particularly of the internet, has transformed learning in recent years. Children and young people need to develop a high level of Computing skills, not only to maximise their potential learning tool, but also to prepare themselves as lifelong learners and for future employment. The internet and other digital and information technologies are powerful tools, which open up new technologies to everyone. Electronic communication helps teachers and pupils learn from each other. These technologies can stimulate discussion and promote creativity and increase awareness of context to promote effective learning. The school has a duty to provide pupils with quality safe internet access as part of their learning experience.

Development, Monitoring and Review of this Policy

This e-safety policy has been developed by the Computing subject leader, the Headteacher and governors.

This e-safety policy was approved by a Governors Sub Committee on:	10.1.17
The implementation of this e-safety policy will be monitored by the:	Senior Leadership Team Computing Subject Leader
Monitoring will take place at regular intervals:	At least once a year.
Due to the ever changing nature of Information and Communication Technologies, the school will review this E- Safety policy annually and, if necessary, more frequently, in response to any significant new developments in the use of technologies, new threats to e-safety or incidents that have taken place. The next anticipated review date will be:	January 2022
Should serious e-safety incidents take place, the following external person will be informed:	South Gloucestershire Safeguarding Officer.

The school will monitor the impact of the policy using:

- A log of reported incidents
- Monitoring logs of internet activity (sites visited and filtered sites)

Scope of the Policy

This policy applies to all members of the school community (including staff, pupils, volunteers, parents/guardians) who have access to and are users of Barrs Court Computing systems.

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 out of school, but is linked to membership of our school.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/guardians of incidents of inappropriate e-safety behaviour that take place out of school.

Roles and Responsibilities

Governors

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. The Computing Link Governor will:

- Regularly monitor e-safety incident logs
- Regularly monitor filtering logs

Headteacher and Senior Management Team

The Headteacher is responsible for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility will be delegated to the E-Safety Coordinator (Computing Subject Leader).

The Headteacher will ensure that the E-Safety Coordinator receive suitable CPD to enable them to carry out their role and train other colleagues as necessary.

SLT will receive regular monitoring reports from the E-Safety Coordinator as appropriate.

The Headteacher and Senior Management Team are aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.

E Safety Coordinators

The E-Safety Coordinators must:

- Take day to day responsibility for E-safety issues and has a leading role in establishing and reviewing the school e-safety policy and related documents.
- Ensure all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- Provide training and advice to staff.
- Liaise with South Gloucestershire Computing team.
- Liaise with school technical staff.
- Receive reports of e-safety incidents and create a log of incidents to inform future e-safety developments.
- Discuss current issues, review incident logs and filtering log with Computing Link Governor as necessary.
- Report to SLT as necessary.

Technical Issues

‘Help Me Help Me’ provides technical and curriculum guidance for e-safety issues.

Internet Provider and Filtering

The South Gloucestershire school internet service is provided by Traded Services and this includes a filtering service to limit access to unacceptable material for all users. Illegal content (child sexual abuse images) is filtered by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. However we are aware that no filtering is completely infallible and consequently focus on teaching pupils to keep safe through our curriculum and teaching. There are two different levels of filtering which are targeted towards different user groups. As a consequence teacher and staff users have access to some resources for teaching that are filtered for learners. Requests from staff for sites to be removed from the filtered list must be approved by the head teacher and this is logged and documented by a process that is agreed by the Head teacher. Any filtering requests for change and issues are reported immediately to the Help Me Help Me technical team. Proactive monitoring is in place via a monitoring box provided by SWGfL. Should anyone attempt to access illegal content this is immediately reported to the police. Illegal activity would include attempting to access:

- child sexual abuse images
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials

Teaching Staff and Support Staff

Teaching staff and support staff are responsible for ensuring that:

- They understand the e-safety policy and practices.
- They have read, understood and signed the Staff Acceptable Use Policy
- They report any suspected misuse or problem to the E-Safety Coordinators (Computing Subject Leaders).
- Digital communication with pupils should be carried out on a professional level and only carried out using official school systems.
- Pupils understand and follow school e-safety policy.
- Pupils have a good understanding of research skills and the need to avoid plagiarism and copyright restrictions.
- They teach to pupils the importance of reporting abuse, misuse or access to inappropriate materials. Teaching time is dedicated to this within the two yearly Computing topic cycle across the whole school. A yearly 'Safer Internet Day' is held each year in February to promote safer and more responsible use of online technology and mobile phones.
- In lessons where the use of internet is pre-planned, pupils are guided to sites that are checked as suitable for their use and should any unsuitable material is found in internet searches information is given to one of the E-Safety coordinators immediately.

Pupils

Pupils should:

- Be responsible for using the school Computing systems in accordance with Pupil Acceptable Use Policy, which their parents/guardians have signed.
- Have a good understanding of research skills and the need to avoid plagiarism and copyright restrictions; they gain this knowledge through direct teaching appropriate to their age.
- Understand the importance of reporting abuse, misuse or access to inappropriate materials. Teaching time is dedicated to this within the two yearly Computing topic cycle across the whole school and through the celebration of the annual Safer Internet Day.
- 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 also applies to their actions out of school.

Parents

Parents and guardians play a crucial role in ensuring that their children understand the need to use the internet and digital technology in an appropriate way. Parents and guardians will be responsible for endorsing (by signature) the Pupil Acceptable Use Policy.

Parent/guardians should:

- Ensure that children access the Internet in a communal room where they can be easily supervised.
- Ensure appropriate supervision for the age of their children including supervising all use of the Internet by younger users.
- Ask their children about what sites they are looking at.
- Ensure that family computers are password protected and have robust anti-virus software which is regularly updated.
- Ensure content is appropriately filtered for younger users.

Rules for Keeping Safe

These are reinforced through the following:

- Pupils sign an acceptable use agreement and this is also communicated to parents who we hope will reinforce the messages at home.
- Pupils are helped to understand the student acceptable use policy and school rules for online safety and encouraged to act accordingly.
- All classes have online safety rules displayed in their classroom and staff regularly refer to these, for example, during activities where children are searching the internet for information. Rules are also displayed in other areas where ICT is used.
- Staff act as good role models in their own use of ICT.
- Staff are aware that there may be some children that are more vulnerable than others to being approached online and endeavour to ensure that these children understand the issues involved.
- Online behaviour is dealt with in accordance with our behaviour policy. There are sanctions and rewards in place for this.

Image Taking by Parents/Legal Guardians or Family Members

- Parents, legal guardians, family members and friends can take images of their child and friends participating in school activities for family and personal use only and agree that any images taken will not be used inappropriately or published on social media sites.
- Parents will be asked for their permission before photography is allowed.

Curriculum

Online safety is now a statutory part of the programme of study for all key stages. Rules and technical solutions are not infallible and we are aware that outside school children will be using unfiltered internet provision. We believe it is crucial to educate children about how to behave responsibly online and how to keep themselves and others safe. Children and young people need the help and support of the school and parents to recognise and avoid e-safety risks. There is a planned and progressive scheme of work for online safety which is taught at every year group. This is based around the Digital Literacy Curriculum by SWGfL and, across the key stages, covers strands on: • Internet safety

- Privacy and security
- Relationships and communication
- Cyberbullying
- Information literacy
- Self image and identity
- Digital footprint and reputation
- Creative credit and copyright

The following aspects also contribute to our curriculum provision:

- Coverage of the experiences is recorded and staff also check understanding when teaching about online safety. • Opportunities to reinforce this are mapped to other subjects in the curriculum where appropriate for example, online behaviour is covered in PSHE and communication, copyright and publishing are referenced in literacy.

- Assemblies are regularly used to reinforce online safety messages.
- Annual online safety events such as Safer Internet Day are also used to raise awareness.

Staff Training and Awareness Raising

There is a planned programme of e-safety training for **all** staff and governors to ensure that they understand their responsibilities, as outlined in this, and the acceptable use policies. The following actions are undertaken to raise awareness:

- An audit of the e-safety training needs of all staff is carried out annually.
- The Child Protection and Online Safety Leader receive regular updates through attendance at relevant training such as SWGfL and LA training sessions and by receiving regular e-safety updates from the South Gloucestershire Traded Services.
- Any reported incidents and how they are addressed are discussed at staff meetings and used as an opportunity to test our processes and update staff on how to deal with issues.
- The E-Safety Leader provides advice/guidance and training as required to individuals and seeks LA advice on issues where appropriate.
- All new staff should receive e-safety guidance as part of their induction programme, ensuring that they fully understand the school E-Safety Policy and Acceptable Use Policies for pupils and staff.
- The Computing / E-Safety Coordinators will receive regular updates through attendance at e-safety conferences and training sessions and by reviewing documents released by BECTA, SWGfL, South Gloucestershire Council and others.

Induction Processes

- All new staff receive e-safety training as part of their induction programme.
- Parents of new reception children receive a briefing about online safety and processes when their child starts school.

There are also updates to this throughout the key stages. A Safer Internet day is held annually.

- Parents of children who join school mid-year are made aware of the processes and their children are also introduced to the acceptable use policy.

Training – Governors

Governors will have opportunities to attend appropriate e-safety training as necessary.

Technical – Infrastructure/Equipment, Filtering and Monitoring The school will be responsible for ensuring:

- That the school infrastructure/network is safe and secure as is reasonably possible and that policies and procedure approved within this policy are implemented. It will also need to ensure that the relevant staff roles named in the above sections will be effective in carrying out their e-safety responsibilities.
- School Computing systems are managed in ways that ensure that the school meets the e-safety technical requirements outlined in SWGfL Security Policy and Acceptable Use Policy and any relevant Local Authority E-Safety Policy and guidance.
- There will be regular reviews of the safety and security of school Computing systems.
- Servers are securely located and physical access restricted.
- All users will have clearly defined access rights to school Computing systems.
- The administrator passwords used by the Network Manager are known by the Computing technical team and can be shared at any time with the Headteacher.
- The school maintains and supports the managed filtering service provided by SWGfL.
- Any filtering issues should be reported immediately to SWGfL.
- Requests from sites to be removed from the filtered list will be considered by technical staff in conjunction with the Headteacher, Computing / E-Safety coordinators and advice from the LA. If the request is granted

this needs to be logged and dated with signatures of the Headteacher and a Computing / E-Safety coordinator.

Reporting and Recording

Because of our duty to all the children, we will take action (such as reporting under-aged profiles and/or contacting the police) if a problem comes to our attention that involves the safety of wellbeing of any of our children.

- There are clear reporting mechanisms in place for online safety incidents and all staff are regularly reminded of these and fully aware of their responsibilities to follow up any reported issues.
- Online safety issues are reported to the Online Safety Lead. If these include allegations of bullying then the antibullying policy is followed.
- Issues which may impact on the well-being and safety of a child are reported directly to the Child Protection Lead and Child Protection procedures are followed.
- Staff who are targeted by bullying online report these issues to the head teacher.
- Any member of staff seeing something online that is negative about the school reports this to the head teacher.
- Pupils are encouraged to report any incidents to an adult whether it relates to themselves or a friend. We encourage children to take responsibility for protecting each other.
- Younger pupils are shown how to use Hector Protector if they access unsafe content and older pupils are also shown how to report online in case of incidents outside school.

  If issues could be a result of problems with infrastructure or may affect it then the technical support provider is informed immediately.
- If access to an unsuitable site is reported then the Online Safety lead will alert the technical support team by contacting Help Me Help Me to ensure that this is blocked.
- Serious incidents are escalated to local authority staff for advice and guidance Jo Briscombe – Curriculum and Policy – 3349

  Safeguarding and Child Protection Officer - 5933
- For incidents affecting school staff the Professionals Online Safety Helpline is contacted for advice if necessary on helpline@saferinternet.org.uk or 0844 381 4772.
- Any reported incidents are logged in the online safety log and followed up in accordance with the relevant policy depending on the issue. The response is also logged and serious issues are followed up after an interval of time to ensure that they are fully resolved.
- There are defined sanctions in place for any breaches of the acceptable use policies. Suggestions for these can be accessed in SWGfL policy template (Word version with appendices) on pages 17 – 19. Schools are advised to adapt these to suit their own circumstances.
- SWGfL provide clear guidance on what to do if there are suspicians that technology may be being mis-used in order to ensure that the right evidence is collected in a way that does not put the school at risk and these are followed. Refer to SWGfL policy template page 20.

Monitoring

- The school will monitor the impact of the policy using:
- • Logs of reported incidents and responses
- • Monitoring logs of internet activity and any network monitoring data
- • Monitoring information about the teaching programme and coverage within the curriculum
- • Regularly checking that pupils and staff are clear about how to report incidents and respond to them
- • The content of the web site is regularly monitored by governors and senior leaders to ensure that it complies with this
- policy and the acceptable use policies.

Use of Digital and Video Images – Photographic, Video

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular, they should recognise the risks attached to publishing their own images on the internet, e.g. on social networking sites.
- Photographs published on the website or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Written permission from parents/guardians will be obtained before photographs of pupils are published on the school website.

Mobile Phones

- The school policy is that pupils are not allowed mobile phones in school. The school phone can be used to contact parents/carers with important messages. Staff are not permitted to use their personal mobile phones to take images of the children.

Social Networking and Personal Publishing

- The school will block/filter access to open social networking sites and give access only to those sites that are monitored and approved by South West Grid recommendations.
- Tools including message boards, blogs, instant messaging and collaboration tools will be used in this safer, closed environment.
- Although pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils, pupils will be taught about the potential risks of social networking sites and what information should not be shared on such sites. The purpose of this is to acknowledge, (although not condone), the reality that some children may already have access to social networking sites by this age.
- See Appendix 3 – Local Authority guidance for parents regarding Social Networking

Data Protection

Staff must ensure that they:

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

Communications Technologies and Social Media

A wide range of communications technologies have the potential to enhance learning and management. The acceptable use agreements outline how these systems should be used.

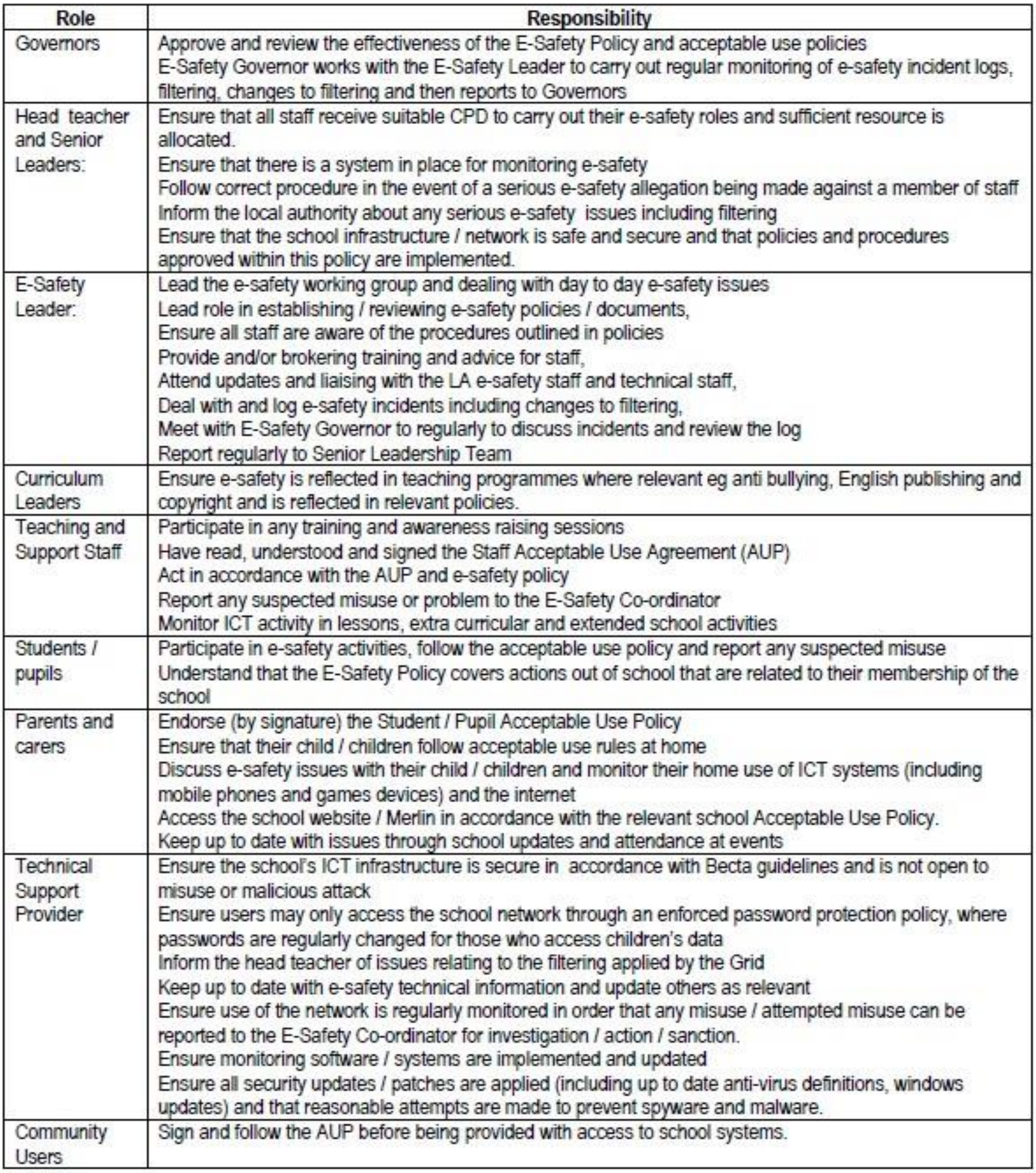
- The official school email service is used for communications between staff, and with parents/carers as it provides an effective audit trail.
- Users are made aware that email communications may be monitored and what to do if they receive an email that makes them feel uncomfortable, is offensive, threatening or bullying in nature through the acceptable use policies. • Personal email addresses, text messaging, public chat and social networking programmes are not be used for communications with parents/carers and children.
- An online secure platform is used for pupil learning and this includes secure access to communications tools so that children can learn about these within a limited environment.

- Personal information is also not posted on the school website and only official email addresses are listed for members of staff. The web site is the responsibility of K.Llewellyn/C.Lester.
- Guidance on personal use of social media and mobile devices is included in the staff, parent and pupil acceptable use
Policies.

Copyright

K.Llewellyn is responsible for making sure that software licence audit is regularly updated and also making regular checks to ensure the number of software installations matches the licences held. Where there are insufficient licences this could breach the Copyright Act which may lead to fines or unexpected additional license costs.

This Online Safety has been agreed by staff and approved by Governors. Due to the ever changing nature of Information and Communication Technologies, the school will review this policy annually and, if necessary, more frequently, in response to any significant new developments in the use of technologies, new threats to e-safety or incidents that have taken place.



Role	Responsibility
Governors	Approve and review the effectiveness of the E-Safety Policy and acceptable use policies E-Safety Governor works with the E-Safety Leader to carry out regular monitoring of e-safety incident logs, filtering, changes to filtering and then reports to Governors
Head teacher and Senior Leaders:	Ensure that all staff receive suitable CPD to carry out their e-safety roles and sufficient resource is allocated. Ensure that there is a system in place for monitoring e-safety Follow correct procedure in the event of a serious e-safety allegation being made against a member of staff Inform the local authority about any serious e-safety issues including filtering Ensure that the school infrastructure / network is safe and secure and that policies and procedures approved within this policy are implemented.
E-Safety Leader:	Lead the e-safety working group and dealing with day to day e-safety issues Lead role in establishing / reviewing e-safety policies / documents, Ensure all staff are aware of the procedures outlined in policies Provide and/or brokering training and advice for staff, Attend updates and liaising with the LA e-safety staff and technical staff, Deal with and log e-safety incidents including changes to filtering, Meet with E-Safety Governor to regularly to discuss incidents and review the log Report regularly to Senior Leadership Team
Curriculum Leaders	Ensure e-safety is reflected in teaching programmes where relevant eg anti bullying, English publishing and copyright and is reflected in relevant policies.
Teaching and Support Staff	Participate in any training and awareness raising sessions Have read, understood and signed the Staff Acceptable Use Agreement (AUP) Act in accordance with the AUP and e-safety policy Report any suspected misuse or problem to the E-Safety Co-ordinator Monitor ICT activity in lessons, extra curricular and extended school activities
Students / pupils	Participate in e-safety activities, follow the acceptable use policy and report any suspected misuse Understand that the E-Safety Policy covers actions out of school that are related to their membership of the school
Parents and carers	Endorse (by signature) the Student / Pupil Acceptable Use Policy Ensure that their child / children follow acceptable use rules at home Discuss e-safety issues with their child / children and monitor their home use of ICT systems (including mobile phones and games devices) and the internet Access the school website / Merlin in accordance with the relevant school Acceptable Use Policy. Keep up to date with issues through school updates and attendance at events
Technical Support Provider	Ensure the school's ICT infrastructure is secure in accordance with Becta guidelines and is not open to misuse or malicious attack Ensure users may only access the school network through an enforced password protection policy, where passwords are regularly changed for those who access children's data Inform the head teacher of issues relating to the filtering applied by the Grid Keep up to date with e-safety technical information and update others as relevant Ensure use of the network is regularly monitored in order that any misuse / attempted misuse can be reported to the E-Safety Co-ordinator for investigation / action / sanction. Ensure monitoring software / systems are implemented and updated Ensure all security updates / patches are applied (including up to date anti-virus definitions, windows updates) and that reasonable attempts are made to prevent spyware and malware.
Community Users	Sign and follow the AUP before being provided with access to school systems.

Pupil Acceptable Use Policy

I have read the E-Safety Policy for Barrs Court Primary School and understand its implications.
I have received the Guide for Parents document and have read and understood its guidance and advice and have shared the information and guidance with my child, (see appendix 1 and 2).

I agree to my child ______________________ having access to the Internet and to Computing systems at school within the framework detailed in the school E-Safety Policy.

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

Signed _________________________

Date_________________

Use of Digital/ Video Images

I agree to the school taking and using digital/video images of my child. I understand that the images can only be used to support learning activities or publicity that reasonably celebrates success and promotes the work of the school.

Signed _________________________

Date_________________

Barrs Court Primary School

Pupil Acceptable Use and E-Safety Policy Agreement

Rationale

The purpose of this policy is to ensure that young learners know how to use the Internet and other technologies responsibly and know what to do if they discover harmful content on the Internet.

Finding Information on the Internet I know:

- That I will get to use the Internet if I use it responsibly, and that being responsible means trying not to visit unsafe sites or registering for things I am not old enough for.
- What to do if I open something I do not like.
- How to search the Internet safely.
- That any information I put on the web can be read by anyone.
- That I should not copy others work and use it as my own.

Using Technology to Contact People I know:

- How to protect my identity and keep my personal information private.
- How to use the safety features of websites.
- That I should be careful who I add as friends online.
- That I need to be polite and friendly online.
- Not to open e-mails if the subject is offensive or if I do not know who it is from.
- What to do if I receive an offensive e-mail/message • That people online may not be who they say they are.

Guide for Parents

Monitoring Home Use of the Internet Parents / carers should:

- Ensure that young people access the internet in a communal room
- Ask their children about what sites they are looking at
- Ensure that family computers are password protected and have robust anti-virus software which is regularly updated
- Ensure content is appropriately filtered for younger users

Content – finding and publishing information on the internet Parents / carers should:

- Ensure that their children know that they will only get to use the internet if they use it responsibly and that being responsible means they should not try to visit unsafe sites or register for things they are not old enough for.
- Ensure that their children know that any protection system does not stop all unsafe content and that children need to tell them if they access something inappropriate.
- Encourage children to search safely to find the information they want and search safely themselves using very specific search terms to reduce the likelihood of accessing unsafe material.
- Supervise younger children when they are using the internet
- Talk to children about the fact that any information published on the web can be read be anyone
- Check information that younger users are publishing on the web before it is posted to ensure that they are not putting themselves in danger

Contact - Using technology to contact people Parents / carers should:

- Discuss user names with children and talk about how to choose them carefully to avoid putting themselves at risk and protect their identity
- Identify the information that young people should keep private in order to prevent them being contacted or traced including
- Talk to children about the need to use safety features of web sites
- Talk to their children about limiting access to their personal information
- That e-mails / messages can be intercepted and forwarded on to anyone
- should talk to their children about being careful who they add as friends
- Talk about the need to be polite online and friendly online and think about the language they use (it could be forwarded to my parents or head teacher!)
- Discuss how to use the subject field in e-mails
- Not to open messages if the subject field contains anything offensive or if I do not recognise who it is from (delete it without opening it)
- Discuss what to do if I receive an offensive message / e-mail including how to keep evidence
- Explain that people online may not be who they seem

Staff (and Volunteer) Acceptable Use Policy

I have read the E-Safety Policy for Barrs Court Primary School and understand its implications.

For my professional and personal safety:

- I understand that the school will monitor my use of Computing systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to the use of school Computing systems out of school.
- I understand that the school Computing systems are for educational use and I will only use the systems for personal or recreational use within the policies and rules set out by school.
- I will not use other usernames and passwords without their express permission.
- I will immediately report any illegal, inappropriate or harmful material or incident I become aware of to the Headteacher or member of SLT.
- I will be professional in my communications and actions when using school Computing systems.
- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will ensure that when I take or publish images of others I do so with their permission (using the most current Pupil Acceptable Use Policy forms signed by parents/ guardians).
- I will only communicate with pupils and parents/guardians using only official school systems.
- I understand that I am responsible for my actions in and out of school. I understand that the Acceptable Use Policy applies not only to my work and use of Computing equipment in school, but also applies to my use of Computing systems and equipment out of school and my use of personal equipment in school.
- I understand that if I fail to comply with the Acceptable Use Policy Agreement I could be subject to disciplinary action.

I have read and understand the above and agree to use the school Computing systems (both in and out of school) and my own devices (in school when carrying out communications related to school) within these guidelines.

Staff/ Volunteer Name: ____

Signed __________________________ Date_____________________

Local Authority guidance for parents on Social Networking

Dear Parent/Carer

Social networking is used everywhere and is a common feature of many people's lives. However if you want to say anything about your child's school or staff on social media there are a few simple guidelines we need to insist you follow, in order to keep all the children in school **safe** and to protect you from possible consequences of your online actions. We already teach the children how to be safe online and you can reinforce this at home by showing your child(ren) how to communicate responsibly online.

Part of our role as a school is to ensure that no confidential information about a child or family is unintentionally disclosed by a parent/carer or a member of staff. There have been several high profile cases in the news when people making offensive comments on social media have been prosecuted.

There are two parts to this brief guidance. The first part is about parent/carer responsibilities. The second is information about what staff are expected to do if they use social media, or come across information about the school (children, parents or staff) on social media.

Guidelines for Parents and Carers

- At all times be respectful of others.
- Never include children's full names (even your own children's).
- Never post or tag photographs etc without ensuring that you have the right permission.
- If there is something you are concerned about in school please contact the school to sort it out rather than discussing it on Facebook for example.
- Everyone who adds to online sites is responsible for any comments posted under their name.
- If you are aware that sites are being misused you have a responsibility to report this.
- If an online conversation looks as if it might be derogatory you should not get involved in the discussion and refer the person to the school.
- You should not accept children as friends on a social networking site.
- If you want to set up a site that refers to your child’s school then please let the school know.
- If you are using social networking sites for school purposes remember that this is a school not personal area so personal comments should not be posted.
- Also if the site is representing the school then please make sure that the good name of the school is preserved and not brought into disrepute.

Staff and Volunteer Responsibilities

- No member of staff or volunteer is allowed to discuss any matter to do with pupils, staff or parents/carers through social media because of safeguarding requirements. This includes tagging photographs etc.
- Some members of staff or volunteers may have social network accounts as a parent or member of a local community group. They must not respond to any comments about the school they come across.
- Staff and volunteers are obliged to inform the school leadership of any concerns they have about comments being made by others.
- Staff have a duty to monitor online spaces and report anything of concern to the school leadership.

The school will always request that any inaccurate or offensive postings are removed. If necessary in an extreme case the school will take legal advice.

Thank you for your understanding and support.