Online Safety Policy including IT Acceptable Use Policy

Non-Statutory Policy (Annual Review)

Governors' Resources Committee

Date next due for review	Date reviewed by Committee	Any Changes YES/NO	Date approved by Committee or Local Academy Board (LAB)
New Policy	14 February 2019	New	

Bracken Leas Primary School
IT Acceptable Use Policy

The designated member responsible for internet safety in the school is Mrs Clare Shannon, Computing and Internet Safety lead.

Aims

The aims of this Acceptable Use Policy are to:

- ensure that pupils benefit from all learning opportunities offered by the internet resources provided by the school in a safe and controlled manner.
- ensure that all staff and students are aware of online risks and are equipped with the necessary skills and knowledge to become responsible digital citizens.
- ensure that all staff benefit from internet access, with clear guidance on safe and acceptable use, both within the school setting and beyond.
- make staff and pupils aware that internet use in school is a resource and a privilege, and if the terms are not met, that the privilege will be taken away.
- provide guidance to staff and pupils about the acceptable use of mobile technologies - both the school's and personal items that are brought into school.

Bracken Leas Primary School computing vision

We view online safety as an integral part of your child's education, therefore online safety units are incorporated into each term so that children learn how to access digital information and use digital media safely and appropriately, both at school and at home. We have regular internet safety assemblies and follow the Google Legends 'Code of being internet Sharp, Alert, Secure, Kind and Brave' in Key Stage 2 and Ask, Think, Check and Tell in Key Stage One and Early Years.

Care of Hardware

If issued, staff must take every care to safeguard their laptop and / or iPad and must not store or leave them unattended in vehicles. It is the user's responsibility to keep their hardware safe and secure at all times and they should not be left unattended. When not in use, the laptop must be stored in the bag provided and kept together with the lead. Any damage, loss or theft of either item must be reported immediately to the IT Coordinator and the School Business Manager.

Purpose of Internet Use

The purpose of internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management information and business administration systems. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils. The statutory curriculum requires pupils to learn computational thinking and programming and associated skills, as well as, how to locate, retrieve and exchange information using IT. In delivering the curriculum, teachers are required to plan to integrate the use of communications technology such as web-based resources and email. Computer skills are vital to access life-long learning and employment; indeed, IT is now seen as an essential life-skill. Internet access is therefore an entitlement for students who show a responsible and mature approach to its use. The school has a duty to provide students with quality internet access as part of their learning experience.

Benefits of using the internet in education include:

- access to world-wide educational resources including museums and art galleries;
- educational and cultural exchanges between pupils world-wide;
- cultural, vocational, social and leisure use in libraries, clubs and at home;
- access to experts in many fields for pupils and staff;

- staff professional development through access to national developments, educational materials and good curriculum practice;
- communication with support services, professional associations and colleagues;
- exchange of curriculum and administration data with the LA and DfES.

Assessing the Risks

Most technologies present risks as well as benefits. Internet use for work, home, social and leisure activities is expanding in all sectors of society. This brings young people into contact with a wide variety of influences, some of which may be unsuitable. Bracken Leas Primary School recognises that it is important to adopt strategies for the safe and responsible use of the internet. In common with other media such as magazines, books, gaming consoles, TV and video, some material available via the internet is unsuitable for pupils. The school will take all reasonable precautions to ensure that users access only appropriate material. The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.

Methods to identify, assess and minimise risks will be reviewed regularly.

The IT Subject Leader will ensure that the internet policy is implemented and compliance with the policy monitored.

However, due to the international scale and linked nature of internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. For this reason, neither the school nor the LA can accept liability for the material accessed, or any consequences of internet access.

Strategies for the safe and responsible use of the internet

The school works in partnership with parents, the LA and DfES to ensure systems to protect pupils are reviewed and improved:

- Filtering strategies are selected by the school, in discussion with the filtering provider where appropriate. The filtering strategy is selected to suit the age and curriculum requirements of the pupils.
- The school internet access is designed expressly for pupil use and includes filtering appropriate to the age of pupils.
- The IT subject leader, alongside the school IT technician, will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- Pupils are taught what internet use is acceptable and what is not and given clear objectives for internet use.
- Internet access is planned to enrich and extend learning activities. Access levels are reviewed to reflect the curriculum requirements and age of pupils.
- Staff will guide pupils in online activities that will support the learning outcomes planned for the pupils' age and maturity.
- Pupils are educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.
- Newsgroups are not made available to pupils.
- Pupils are not allowed access to public or any chat rooms.

Evaluation of Internet Content

- If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Internet Service Provider via the IT Leader. This information will be passed on to the IT subject lead and reviewed regularly.
- Any material that the school believes is illegal must be referred to the Internet Watch Foundation.
- Users must ensure that the use of internet derived materials complies with copyright law.
- Pupils are taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

- Pupils are taught to search for public domain stock images, acknowledge the source of information used and to respect copyright when using internet material in their own work.

Use of Email

Although our children do not have school email accounts, the government encourages the use of email as an essential means of communication for both staff and pupils. Directed email use can bring significant educational benefits and interesting projects. However, unregulated email can provide a means of access to a pupil that bypasses the traditional school boundaries. In the school context, therefore, email is not considered private and maybe monitored by staff, whilst trying to achieve a balance between monitoring that is necessary to maintain the safety of pupils and the preservation of human rights, both of which are covered by recent legislation.

- The school email system is to be used for school business
- Staff should use their school email account for school business
- Pupils may only use school-provided email accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive email and will be encouraged to maintain it as evidence.
- Pupils must not reveal details of themselves or others in email communication, such as address or telephone number, or arrange to meet anyone.
- Pupils may not access home email accounts in school.
- Email sent to an external organisation is written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- The sending of abusive or inappropriate email messages is forbidden.

Management of Website Content

The school website is a virtual space to promote the school and celebrate pupils' work and achievements

- The point of contact on the website is the school address, school email and telephone number. Staff or pupils' home information are not to be published.
- Pupils' full names are not be used on the website, particularly in association with photographs.
- Written permission from parents or carers is obtained before photographs of pupils are published on the school website.
- The Headteacher, Assistant Head, IT subject leader and nominated office staff take overall editorial responsibility and try to ensure that content is accurate and appropriate.
- The copyright of all material is held by the school, or be attributed to the owner where permission to reproduce has been obtained.

Procedures for Use of Video and Photographs

The term 'image' refers to the taking of video footage or photographs via any camera or other technology, e.g. a mobile phone. When in school there is access to:

- Video cameras
- iPad
- Digital cameras

These are all located within the IT room, office or individual classrooms.

Staff should avoid, where possible, the use of their own personal equipment for taking photos. Occasionally, photos may be taken e.g. for immediate communication via the school Twitter account, however, all photo content stored on the device must be deleted as soon as possible after return to school, where it must be stored centrally. Content should be taken for legitimate school purposes only.

The sharing of photographs via weblogs, forums or any other means online is only permitted through school designated platforms.

Any photographs or video clips uploaded for school purposes should not have a file name of a child, especially where these may be uploaded to a school website. Photographs should only ever be included if the parents/carers have signed the permission slip indicating they give permission for their names to be used. A record of signed permissions is kept in the office and in individual pupil records.

Children should not be photographed in compromising positions or in inappropriate clothing. Photographs of school children should only be stored on school equipment, such as school USBs, school laptop hard drives or the school network.

Video-conferencing and Webcams

Taking images via a webcam should follow the same procedures as taking images with a digital or video camera.

Permission will be sought from parents and carers if their child is engaged in video conferencing with individuals or groups outside of the school setting. This process should always supervised by a member of staff and a record of dates, times and participants held by the school.

Pupils need to tell an adult immediately of any inappropriate use by another child or adult.

Managing Emerging Internet Applications

Many emerging communications technologies offer the potential to develop new teaching and learning tools. Mobile communications, wide internet access and multimedia present opportunities that need to be evaluated to assess risks, to establish benefits and to develop good practice. Emerging technologies will be examined for educational benefit and evaluated before use in school is allowed.

Mobile Phones and other Emerging Mobile Technologies

Bracken Leas Primary School has considered carefully how the use of mobile technologies can be used as a teaching and learning tool within the curriculum.

The following areas of concern must be taken into consideration:

- inappropriate or bullying text messages,
- images or video taken of adults or peers without permission being sought,
- the videoing of violent or abusive acts towards a child, young person or adult which is often distributed,
- the sending of suggestive or sexually explicit personal images via mobile phones.

As a result of this, Bracken Leas Primary School does not allow pupils to keep mobile phones in their possession at school. Any child who does bring a mobile phone into school must hand it in to their class teacher for its safekeeping (the child is responsible for their phone at all times). Phones should never be used by pupils on school grounds – including before and after school clubs.

Guidance for Staff

Personal Mobile Devices

Staff are allowed to bring in personal mobile phones or devices for their own use, but **must not use personal numbers to contact children and young people under any circumstances nor must they ever give out their own personal phone number / mobile number/ email address or engage in any exchange with pupils / ex pupils using social networking facilities (in accordance with the school Code of Conduct).**

- Staff must ensure that there is no inappropriate or illegal content stored on the device and should be aware that using features, such as video or sound recording, may be subject to the same procedures as taking images from digital or video cameras.

- If personal mobile phones are used to take photographs for legitimate school / educational purposes, they should be transferred to school storage systems and deleted from personal devices as soon as possible: school images should not be stored on personal devices.
- Staff should be aware that games consoles such as the Sony PlayStation, Microsoft Xbox and other such systems have internet access which may not include filtering. Before use within school, authorisation should be sought from the Headteacher and the activity supervised by a member of staff at all times.
- The school is not responsible for any theft, loss or damage of any personal mobile device.

School/Educational Establishment Issued Mobile Devices and Email

The management of the use of these devices and facilities should be similar to those stated above, but with the following additions:

- As a point of principle, school allocated equipment should be used for school business whenever possible.
- We discourage, not prohibit, personal material being stored on the laptops and/or iPads allocated to staff. However, staff should be aware that the Employee's use of the telephone, PC, email and internet systems may be monitored from time to time by the Employer and you do not, therefore, have an expectation of privacy. Such monitoring will be for legitimate purposes including without limitation the ensuring of compliance with statutory and legal requirements and the rules and procedures (especially Safeguarding / Professional Standards and Code of Conduct) from time to time in force. Failure to comply with the Employer's procedures on email and internet use may be a disciplinary offence under the Disciplinary Procedures.
- Although personal use of email facilities is discouraged, *limited* personal use will be permitted provided that the content of messages is appropriate, i.e. is not likely to cause offence. Staff and students should regard this facility as a privilege that should normally be exercised in their own time without detriment to the job or study and not abused. Inappropriate or excessive use may result in disciplinary action and/or removal of facilities. However, staff should be aware that both private and business use of email will be subject to monitoring or access by senior staff if necessary. Staff must be aware of confidentiality issues and must not communicate to the public, press, television or any outside agency the contents of any documents relating to the Employer.

Social Networking Advice for Staff

Social networking outside of work hours, on non school-issue equipment, is the personal choice of all school staff. Owing to the public nature of such websites, it is advisable for staff to consider the possible implications of participation. The following advice should be considered if involved in social networking:

- Personal details are never shared with pupils such as private email addresses, telephone numbers or home addresses. It is recommended that staff ensure that all possible privacy settings are activated to prevent students from making contact on personal profiles. The simplest and most effective way to do this is to use a pseudonym, remove details from search results and turn off public visibility.
- Staff should not engage in personal online contact with pupils or parents outside of Headteacher authorised systems (e.g. school email account for homework purposes)
- Staff should ensure that the highest privacy settings are in place to prevent students from accessing photo albums or personal information.
- Staff are advised against accepting invites from colleagues until they have checked with them in person that the invite is genuine (avoiding fake profiles set up by students).
- Staff should not publish any pictures / images of other colleagues, or their families, in in-school or out of school settings without their permission.

Authorisation of Internet Access

The school allocates internet access for staff and pupils on the basis of educational need.

- All pupils accessing the internet on school computers are directly supervised by a member of staff.

How is the Policy Introduced to Pupils?

- Rules for internet access are located with the laptops and Key Stage one computing area and are acknowledged as part of the log on process.
- Pupils are informed that internet use will be monitored.
- Pupils are instructed in responsible and safe use.
- Lessons on responsible internet use will be included in IT lesson time at the beginning of each module requiring access to the school web.
- Termly assemblies will take place in the policy message will be reinforced.

Staff Internet Use

- All staff must accept the terms of this policy before using any internet resource in school.
- All staff including teachers, supply staff, classroom assistants and support staff, will be provided with the School Internet Policy, and are required to sign to show acceptance of the rules.
- Staff should be aware that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff are aware that under no circumstances should they be in contact with pupils other than for Headteacher authorised school business.
- The monitoring of internet use is a sensitive matter. Monitoring procedures are supervised by the Headteacher / IT subject leader.

Appropriate and Inappropriate Use of the Internet by Staff

Staff members have access to the network so that they can obtain age appropriate resources for their classes and create folders for saving and managing resources.

They have a password on laptops to access a filtered internet service and know that this should not be disclosed to anyone or leave a computer or other device unattended whilst they are logged in.

All staff will have access to Acceptable Use Policy. A register of Annual acceptance of these rules is kept in the office.

In the Event of Inappropriate Use

If a member of staff is believed to misuse the internet or learning platform in an abusive or illegal manner, a report must be made to the Headteacher immediately.

Inappropriate Use by Children or Young People

Acceptable Use Rules for children, young people and parents/carers are outlined in the appendices. These detail how children and young people are expected to use the internet and other technologies within school or other settings, including downloading or printing of any materials. The rules are there for children and young people to understand what is expected of their behaviour and attitude when using the internet which then enables them to take responsibility for their own actions. For example, knowing what is polite to write in an email to another child, or understanding what action to take should there be the rare occurrence of sighting unsuitable material. This also includes the deliberate searching for inappropriate materials and the consequences for doing so.

The rules should be on display within the classrooms, in teaching areas and in locations where there are computer charging stations/storage trolleys, where this may be applicable.

Bracken Leas Primary School will encourage parents/carers to support the rules with their child or young person. This can be shown by signing the Acceptable Use Rules together so that it is clear to the school or setting that the rules are accepted by the child or young person with the support of the parent/carer. This is also intended to provide support and information to parents/carers when children and young people may be using the internet beyond school.

Further to this, it is hoped that parents/carers will add to future rule amendments or updates to ensure that they are appropriate to the technologies being used at that time and reflect any potential issues that parents/carers feel should be addressed, as appropriate.

The downloading of materials (for example, music files and photographs) need to be appropriate and 'fit for purpose' based on research for work and be copyright free.

File-sharing via email, weblogs or any other means online should be appropriate and be copyright free when using the learning platform in or beyond school.

In the Event of Inappropriate Use by Children

Should a child or young person be found to misuse the online facilities whilst at school the following consequences will occur:

- Any child found to be misusing the internet by not following the Acceptable Use Rules may have a letter sent home to parents/carers explaining the reason for suspending the child or young person's use for a particular lesson or activity.
- Further misuse of the rules may result in not being allowed to access the internet for a period of time and another letter will be sent home to parents/carers.
- A letter may be sent to parents/carers outlining the breach in Child Protection Policy where a child or young person is deemed to have misused technology against another child or adult.

In the event that a child or young person **accidentally** accesses inappropriate materials the child should report this to an adult immediately and take appropriate action to hide the screen or close the window. The issue of a child or young person deliberately misusing online technologies should also be addressed by the establishment.

Children should be taught and encouraged to consider the implications for misusing the internet and posting inappropriate materials to websites, for example, as this may have legal implications.

Nationally there have been concerns about pupils gaining access to undesirable materials. We have taken positive steps to deal with this risk at school. Our Internet service provider operates a school standard filtering system that restricts access to inappropriate materials.

Whilst every endeavour is made to ensure that suitable safeguarding restrictions are in place to prevent the ability of children to accessing inappropriate materials, please note that the Local Academy Board will not be held liable under any circumstances for any damages arising from your child's use of the Internet facilities.

Maintaining IT System Security

The school IT systems will be reviewed regularly with regard to security.

- Virus protection and Firewalls for the whole network are installed and expected to be kept current.
- All portable media (laptops), which carry personal school or pupil information, are password protected or encrypted for data protection purposes in the event of loss or theft. No pupil / school data should be carried on memory sticks.
- Uploading and downloading of non-approved software is not permitted onto school equipment.
- Computers should only be used for schoolwork and homework unless permission has been granted otherwise.

- No programs on disc or USB/Memory Stick/Flash drive should be brought in by pupils from home for use in school although staff can seek permission from the Head. This is for both legal and security reasons.
- Unapproved system utilities and executable files are not be allowed in pupils' work areas or attached to email.
- The IT subject leader / our IT support will ensure that the system has the capacity to take increased traffic caused by internet use.

How is Parent/Carer Support Enlisted?

Internet use in pupils' homes is increasing rapidly, encouraged by offers of free access and continual media coverage. Unless parents/carers are aware of the dangers, pupils may have unrestricted access to the internet. The school can support parents/carers plan appropriate, supervised use of the internet at home. Parents/carers are also advised to check if pupils' use of the internet elsewhere, such as libraries, is covered by an appropriate use policy.

- Parents'/ carers' attention will be drawn to the School Internet Policy in newsletters, the school brochure and on the school website.
- Internet issues will be handled sensitively to inform parents/ carers without undue alarm.
- A partnership approach with parents is encouraged.
- Advice on filtering systems, home hub controls and educational and leisure activities that include responsible use of the internet is available to parents/carers.

Bracken Leas Primary School Pupil Internet and IT Agreement

- At Bracken Leas Primary School, we expect all pupils to be responsible for their own behaviour on the internet, just as they are anywhere else in school.
- This includes materials they choose to access, and language they use.
- Pupils need to tell an adult immediately of any inappropriate use of IT.
- Pupils using the internet are expected not to deliberately seek out offensive materials. Should any pupils encounter any such material accidentally, they are expected to report it immediately to a teacher.
- Pupils are expected not to use any inappropriate language in their email communications and contact only people they know or those the teacher has approved.
- Pupils must ask permission before accessing the internet in school.
- Pupils should not access other people's files unless permission has been given.
- School equipment should only be used for schoolwork and homework unless permission has been granted otherwise.
- No program files may be downloaded to the computer from the internet.
- No programs on memory stick or CD Rom should be brought in from home for use in school without the approval of a teacher
- Personal printing is not allowed on our network for cost reasons (e.g. pictures of pop groups/cartoon characters).
- No personal information (such as name, phone numbers and addresses should be given out and no arrangements to meet someone made unless this is part of an approved school project.
- Pupils consistently choosing not to comply with these expectations will be warned, and subsequently, may be denied access to internet resources.
- Mobile phones must be handed in to your child’s class teacher upon arrival at school and collected at the end of the day for safekeeping.
- Personal cameras / video equipment should not be brought in to school.

Bracken Leas Primary School Staff Acceptable Use Policy

- Staff must at all times be aware of the requirements of the Data Protection Act 1998 and act accordingly. This includes, but is not restricted to, meaning that you must keep personal data secure, and explicitly forbids you from emailing documents to your personal email accounts or other unauthorised third parties

- Staff using the internet are expected not to deliberately seek out offensive materials. Should any staff encounter any such material accidentally, they are expected to report it to the IT Subject Leader who will arrange to adjust the school filtering system

- Staff must ensure that they leave school devices (e.g. laptops; tablets) logged off to prevent unauthorised access to content and user accounts.

- Staff are expected not to use any inappropriate language in their email communications and treat such communications as they would a letter on headed paper. All communication with parents/carers must go through approved channels via the office / headteacher.

- Personal use of email facilities is discouraged, however, *limited* personal use will be permitted.

- Staff must be aware of confidentiality issues and must not communicate to the public, press, television or any outside agency the contents of any documents relating to the Employer.

- We discourage, not prohibit, personal material being stored on the laptops/iPads allocated to staff. However, staff should be aware that the Employee's use of the telephone, PC, email and internet systems may be monitored.

- Staff should keep personal content on school devices (e.g. laptop) to a minimum, and all personal content should be backed up on personal storage devices at home (e.g. an external disk drive or a cloud service). Personal photos / videos should not be stored on any school device (eg laptops / tablets).

- School-related content stored on any personal device (such as photos/movies) must be deleted as soon as possible after return to school, where it must be stored centrally.

- Staff should ensure that all equipment for which they are responsible is kept securely and treated with care.

- No program files may be downloaded to any computer from the internet without permission from the IT Subject Leader.

- Memory sticks/ external hard drives brought in from home for use in school should be virus checked before use and password protected to maintain the privacy of any personal information saved on them. No confidential information / data should be transported on memory sticks.

- Mobile phones should be kept in a secure place away from pupils and should not be accessed during teaching times.

- Staff must not make contact with parents or pupils using personal phones / email or give out phone numbers/ personal email addresses. Contact with parents/ carers when offsite, on school business can either be done via the school office

- Staff should not publish any pictures / images of other colleagues, or their families, in in-school or out of school settings without their permission.

- Staff should ensure that the highest privacy settings are in place to prevent students from accessing photo albums or personal information.

- Staff are advised against accepting invites from colleagues until they have checked with them in person that the invite is genuine (avoiding fake profiles set up by students).

- All staff are obligated to report misuse by pupils / staff.

- Personal printing is not allowed on our network for cost reasons.