Broad Oak Primary School

E-SAFETY POLICY
(incl. Acceptable Use)

December 2019

Broad Oak Primary School
E-Safety Policy

'Pupils have the right to come to school and focus on their studies, free from disruption and the fear of bullying,' The White Paper 2010.

At Broad Oak we want all children and staff be treated as individuals. The Single Equality Act 2010 covers the 9 equality strands defined as protected characteristics: age; disability; gender assignment; marriage and civil partnership; pregnancy and maternity; race; religion or belief; sex; sexual orientation. In this school we will ensure that at every level, in all of our work and throughout all aspects of school community and its life, all will be treated equally. We will promote and strive for inclusive education through the promotion of our Core Values and British Values and our work towards the Unicef Rights Respecting School Award.

(This policy is to be read in conjunction with the Behaviour Policy, Anti-Bullying Policy, SEND policy and Safeguarding Policy.

New technologies inspire children to be creative, communicate and learn. However, while the internet is a great resource, it is important that children and young people are protected from the risks they may encounter. Appleton Primary School endeavours to highlight benefits and risks of using technology and provides Safeguarding and education for users to enable them to control their online experience.

Links to national guidance

The following local/national guidance should also be read in conjunction with this policy:

- PREVENT Strategy HM Government
- Keeping Children Safe in Education DfE September 2019
- Teaching Online Safety in Schools DfE June 2019
- Working together to Safeguard Children
- Learning together to be Safe: A Toolkit to help Schools contribute to the Prevention of Violent Extremism.

Learning and Teaching

We believe that the key to developing safe and responsible behaviours online, not only for pupils but everyone within our school community, lies in effective education. We know that the internet and other technologies are embedded in our pupils' lives, not just in our school but outside as well, and we believe we have a duty to help prepare our pupils to safely benefit from the opportunities the internet brings.

We will provide a curriculum (incl. Junior Jam) which has e-Safety related lessons embedded throughout.

- We will celebrate and promote e-Safety through a planned programme of assemblies and whole-school activities, including promoting Safer Internet Day each year.
- We will discuss, remind or raise relevant e-Safety messages with pupils routinely wherever suitable opportunities arise during all lessons; including the need to protect personal information, consider the consequences their actions may have on others, the need to check the accuracy and validity of information they use and the need to respect and acknowledge ownership of digital materials.
- Any internet use will be carefully planned to ensure that it is age appropriate and supports the learning objective for specific curriculum areas.
- Pupils well be taught how to use a range of age-appropriate online tools in a safe and effective way.
- We will remind pupils about their responsibilities through an Acceptable Use Policy which every pupil will sign and be displayed throughout the school.
- School will model safe and responsible behaviour in their own use of technology during lessons.
- We will teach pupils how to search for information and to evaluate the content of websites for accuracy when using them in any curriculum area.

- When searching the internet for information, pupils will be guided to use age- appropriate search engines. All use will be monitored and pupils will be reminded of what to do if they come across unsuitable content.
- Pupils will be taught about the impact of online bullying and know how to seek help if they are affected by any form of online bullying. (See Anti-Bullying Policy).
- Pupils will be made aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent or carer, teacher or trusted staff member, or an organisation such as Childline or the CEOP report abuse button.

Staff Training

Our staff receive regular information and training on e-Safety issues, as well as updates as and when new issues arise.

- As part of the induction process all staff receive information and guidance on the e- Safety Policy, the school's Acceptable Use Policy, e-security and reporting procedures.
- All staff will be made aware of individual responsibilities relating to the safeguarding of children within the context of e-safety and know what to do in the event of misuse of technology by any member of the school community.

Managing ICT Systems and Access

- The school will agree on which users should and should not have internet access and the appropriate level of access and supervision they should receive
- All users will be made aware that they must take responsibility for their use and behaviour while using the school ICT system and that such activity will be monitored and checked.
- At Key Stage 1, pupils will access the network using an individual username and a class password which the teacher supervises (JJ / TTRS).
- At Key Stage 2, pupils will have an individual user account with an appropriate password which will be kept secure, in-line with the pupil Acceptable Use Policy. They will ensure that they log out after each session (JJ/ TTRS/ RP).
- All internet access will be undertaken alongside a member of staff or, if working independently, a member of staff will supervise at all times.
- Members of staff will access the internet using an individual ID and password, which they will keep secure. They will ensure that they log out after each session and not allow pupils to access the internet through their ID or password. They will abide by the school AUP at all times.

Managing Filtering

- The school has the Baracuda filtering system in place which is managed by the school and Computeam. Banned phrases and websites are identified.
- The school has a clearly defined procedure for reporting breaches of filtering. All staff and pupils will be aware of this procedure by reading the Acceptable Use Policy and by attending the appropriate awareness training/online safety lesson
- If staff or pupils discover an unsuitable site, it must be reported to the e-Safety Co- ordinator immediately.
- If users discover a website with potentially illegal content, this should be reported immediately to the e-Safety Co-ordinator. The school will report such incidents to appropriate agencies including Internet Service Provider (ISP), Police, CEOP or the Internet Watch Foundation (IWF).
- Any amendments to the school filtering policy or block and allow lists will be checked and assessed by the e-Safety Co-ordinator prior to being released or blocked.
- The evaluation of online content materials is a part of teaching and learning in every subject and will be viewed as a whole-school requirement across the curriculum.

E-Mail

- Staff should only use approved email accounts allocated to them by the school and should be aware that any use of the school email system will be monitored and checked.
- Staff should not use personal email accounts for professional purposes, especially to exchange any school related information or documents or to email parents/carers.
- Staff should not send emails to pupils.
- Irrespectively of how staff access their school email (from home or within school), school policies still apply.
- Chain messages are not permitted or forwarded on to other school owned email addresses.

Social Networking

- Staff will not post content or participate in any conversations which will be detrimental to the image of the school. Staff who hold an account should not have parents or pupils as their 'friends'.
- School blogs or social media sites should be password protected and run from the school website with approval from the Senior Leadership Team.

Pupils Publishing Content Online

- Pupils will not be allowed to post or create content on sites unless the site has been approved by a member of the teaching staff.
- Pupils' full names will not be used anywhere on the website, particularly in association with photographs and video.
- Written permission is obtained from the parents/carers before photographs and videos are published.
- Any images, videos or sound clips of pupils must be stored on the school network and never transferred to personally-owned equipment.
- Pupils and staff are not permitted to use portable devices to store images/video/sound clips of pupils.

Mobile Phones and Devices General use of personal devices

- Staff mobile phones and personally-owned devices will not be used in any way during lessons. They should be switched off or silent at all times.
- No images or videos will be taken on mobile phones or personally owned devices.
- In the case of school productions, Parents/carers are permitted to take pictures of their child in accordance with school protocols which strongly advise against the publication of such photographs on social networking sites.
- The sending of abusive or inappropriate text, picture or video message is forbidden.

Pupils' use of personal devices

- Pupils' who need to bring a mobile phone in to school can only do so if a written request is received from parents explaining the reason that a mobile phone would be needed. The mobile phone must be handed in to the school office on arrival and collected at the end of the day.
- Pupils who do not follow the school policy relating to the use of mobile phones will not be permitted to bring their mobile phones into school.

Screening,Searching and Confiscation

The Education Act 2011, allows staff to lawfully search electronic devices, without consent or parental permission, if there is a suspicion that the pupil has a device prohibited by school rules, or the staff member has good reason to suspect the device may be used to:

- cause harm,
- disrupt teaching,
- break school rules,
- commit an offence,
- cause personal injury, or
- damage property.

Staff use of personal devices

- Staff are not permitted to use their own mobile phones or devices for contacting children or their families within or outside of the setting in a professional capacity.
- Staff will not use personal devices such as mobile phones or cameras to take photos or videos of pupils and will only use school provided equipment for this purpose.
- If a member of staff breaches the school policy then disciplinary action may be taken.
- Mobile phones and personally -owned devices will be switched off or switched to 'silent' mode, Bluetooth communication should be 'hidden' or switched off and mobile phones or devices will not be used during teaching periods unless permission has been granted by a member of the senior leadership team in emergency circumstances.

CCTV

- The school may use CCTV in some areas of school property as a security measure.Cameras will only be used in appropriate areas and there is clear signage indicating where it is in operation.

General Data Data Protection (GDPR) and e-safety

Data must always be processed lawfully, fairly and transparently; collected for specific, explicit and legitimate purposes; limited to what is necessary for the purposes for which it is processed; accurate and kept up to date; held securely; only retained for as long as is necessary for the reasons it was collected.

GDPR is relevant to e-safety since it impacts on the way in which personal information should be secured on school networks, computers and storage devices; and the security required for accessing, in order to prevent unauthorised access and dissemination of personal material.

Staff need to ensure that care is taken to ensure the safety and security of personal data regarding all of the school population and external stakeholders, particularly, but not exclusively: pupils, parents, staff and external agencies.

Personal and sensitive information should only be sent by e mail when on a secure network. Personal data should only be stored on secure devices.
In the event of a data breach, the school will notify the Data Protection Officer (DPO) immediately, who may need to inform the Information Commissioner's Office (ICO).

Authorising Internet access

- All staff must read and sign the 'Acceptable Use Policy' before using any of school ICT resources.
- All parents will be required to sign the home-school agreement prior to their children being granted internet access within school.
- All visitors will be asked to read the Acceptable User Policy prior to being given internet access within the school.
- The school will maintain a current record of all staff and pupils who have been granted access to the school's internet provision.

Support for Parents

- Parents attention will be drawn to the school's e-Safety policy and safety advice in newsletters, the school website and e-Safety information workshops.

- The school website will be used to provide parents with timely and meaningful information about their children's school lives and work to support the raising of achievement. The website will also provide links to appropriate online-safety websites.

Radicalisation Procedures and Monitoring

It is important for us to be constantly vigilant and remain fully informed about the issues which affect the region in which we teach. Staff are reminded to suspend any professional disbelief that instances of radicalisation 'could not happen here' and to refer any concerns through the appropriate channels (currently via the DSL). Regular monitoring and filtering is in place to ensure that access to appropriate material on the internet and key word reporting it in place to ensure safety for all staff and pupils.

Sexual Harassment

Sexual harassment is likely to: violate a child's dignity, make them feel intimated, degraded or humiliated and/or create a hostile, offensive or sexualised environment.

Online sexual harassment, which might include non-consensual sharing of sexual images and videos and sharing sexual images and videos (both often referred to as 'sexting'; inappropriate sexual comments on social media; exploitation; coercion and threats).

Any reports of online sexual harassment will be taken seriously, and the police and Manchester Contact Centre may be notified.

Our school follows and adheres to the national guidance - UKCCIS: Sexting in schools and colleges: Responding to incidents and safeguarding young people

Responses to Incident of Concern

An important element of e-Safety is the ability to identify and deal with incidents of concern including the confidentiality of information. All staff, volunteers and pupils have a responsibility to report e-Safety incidents or concerns so that they may be dealt with effectively and in a timely manner in order to minimise any impact. The school has incident reporting procedures in place and record incidents of an E-Safety nature on C-poms.

Sanctions

Misuse of the Internet may result in disciplinary action, including written warnings, withdrawal of access privileges, and in extreme cases, exclusion, in accordance with the school's Behaviour Policy. The school also reserves the right to report any illegal activities to the appropriate authorities

Policy Review Date: December 2020 or when changes are necessary to comply with school policy or national legislation.

Broad Oak Primary School

All Staff, Student and Volunteer Acceptable Use Policy

School Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for students/volunteers to be more creative and productive in their work. All users should have an entitlement to safe access to the internet and digital technologies at all times.

This Acceptable Use Policy is intended to ensure:

- that all adults will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that all adults are protected from potential risk in their use of technology in their everyday work.

The school will try to ensure that adults will have good access to digital technology to enhance their work, to enhance learning opportunities for *students / pupils* learning and will, in return, expect students/volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that students / pupils receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

For my professional and personal safety:

- I understand that Broad Oak Primary School will monitor my use of the school digital technology and communications systems.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email etc.) out of school, and to the transfer of personal data (digital or paper based) out of school.
- I understand that the school digital technology 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.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using *Broad Oak Primary School's* 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 ensure that when I take and / 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 / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the school website) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use social networking sites in school in accordance with the school's policies.
- I will only communicate with parents / carers using official school systems. Any such communication will be professional in tone and manner
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school have the responsibility to provide safe and secure access to technologies and ensure the smooth running of Broad Oak Primary School:

- When I use my mobile devices (laptops / tablets / mobile phones) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. 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 email addresses on the school ICT systems without seeking permission.
- I will not use USB devices whilst at the school.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will ensure that my data is regularly backed up.
- 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 such 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 from 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 / academy 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. Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based protected and restricted data must be held in lockable storage.
- I understand that data protection policy requires that any 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 / academy policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

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

- I understand that this Acceptable Use Policy applies not only to my work and use of school digital technology equipment in school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises 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 include a warning, a suspension, referral to Governors / Directors and / or the trust/university and in the event of illegal activities the involvement of the police.

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

Name:……..

Position in school:……..

Signed:…….

Date:……