BRICKNELL PRIMARY SCHOOL

Online Safety Policy

e-Safety Co-ordinator – Matthew Mullen
ICT Co-ordinator – Matthew Mullen
Safeguarding Governor – Michele Colthup

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. Bricknell Primary School endeavors to highlight the benefits and risks of using technology and provides safeguarding and education for users to enable them to control their online experience.

Links to other policies and national guidance

The following school policies and procedures should also be referred to

- Child Protection and Safeguarding Policy
- Whistleblowing Policy
- Behaviour Policy
- Guidance on Safer Working Practice
- Anti-bullying Policy

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

- Hull Safeguarding Children's Partnership, Guidelines and Procedures
- PREVENT Strategy HM Government
- Keeping Children Safe in Education DfE September 2019
- Working Together to Safeguard Children HM March 2018

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 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 broad and balanced curriculum which has online safety related lessons embedded throughout
- We will celebrate and promote online safety through a planned progressive curriculum, including promoting Safer Internet Day each year.
- Weekly Safeguarding assemblies take play across the school to embed safeguarding messages and reinforce safety information to the children.
- We will discuss, remind or raise relevant online 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 objectives for specific curriculum areas.
- Pupils will 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 tick to say they have read and understood each time they log on to any computer within school. This information is shared with the children at the beginning of each academic year (See appendices 1 and 2)
- Staff 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 online safety issues, as well as updates as and when new issues arise.

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

Managing ICT Systems and Access

- The school will agree which users should and should not have internet access and the appropriate level of access and supervision they should receive.
- All users will sign an Acceptable Use Policy provided by the school, appropriate to their age and type of access on logging on to the computers within the school. Users will be made aware that they must take responsibility for their use and behaviour while using the school ICT systems and that such activity will be monitored and checked.
- Any visitors to the school who require access to the computers will have student level access only and be monitored in line with the school system.
- At Key Stage 1, pupils will access the network using an individual username and a class password, which the teacher supervises.
- 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 they log out after each session.
- 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 and password. They will abide by the school AUP at all times.

Managing Filtering

- The school has a Smoothwall filtering system in place which is managed by the school and RM. Banned phrases and websites are identified.
- The school has a clearly defined procedure for reporting breaches of filtering.
- The IT systems are all monitored by eSafe monitoring systems which send weekly reports and identify any breaches immediately. Any breaches are immediately sent to the Head of School for immediate investigation.
- If staff or pupils discover an unsuitable site with possible illegal content, it must be reported to the e-Safety Co-ordinator immediately. This will then be reported to RM to be blocked through Smoothwall. The school will report such incidents to appropriate agencies including the ISP, Police, CEOP or the IWF.
- Any amendments to the school filtering policy or block-and-allow lists will be checked and assessed by the head of school/e-Safety Coordinator prior to being released or blocked.

E-Mail

- Staff and pupils 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.
- Pupils are encouraged to immediately tell a teacher or trusted adult if they receive any inappropriate or offensive emails.
- Irrespective of how pupils or 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 inappropriate 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’. Doing so will result in disciplinary action or dismissal.
- 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/blog, particularly in association with photographs and video.
- Written permission is obtained from parents/carers annually 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.

General use of personal devices

- Staff will not use their mobile phone internet data to access to circumvent school policy.
- Mobile phones and personally-owned devices will not be used in any way during lessons or school time. 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 photographs of their own child in accordance with school protocols which strongly advise against the publication of any 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 into school can only do so if a written request is received from parents explaining the reason that a mobile phone is needed.
- Parents sign an agreement that states that they have discussed the appropriate use of mobile phones with their child. This reinforces the rule that mobile phones will be switched off as soon as the pupil enters the school building and will be taken to the office for safe keeping. They must not be kept in classrooms or lockers.
- 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.

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.

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.

Sanctions

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

Online 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 Children's Social Care 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.*

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 Child Protection/ Safeguarding Co-ordinator). Regular monitoring and filtering is in place to ensure that access to inappropriate material on the internet and key word reporting is in place to ensure safety for all staff and pupils

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.

Authorising Internet access

- All staff must read and accept 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 and students will be asked to read and sign the Acceptable Use Policy prior to being given internet access within the school.

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.

Response to an 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.

Governing Body

The Governing Body are fully informed of the monitoring and Filtering systems in place and are provided with termly updates on the number of incidents. The Governing Body are made aware of any breaches to this policy.

Appendix 1

Bricknell Primary School
Acceptable Use Policy - Staff

1. STATEMENT OF POLICY

The Academy believes that the internet is an important and valuable tool and that the ability to use it is a key skill for the 21st century. The Academy is a learning community and it is therefore the Board of Director's intention to support all staff in developing the confidence and ability to access the internet, whilst ensuring that provisions are in place to prevent abuse.

THIS POLICY MUST BE READ IN CONJUNCTION WITH THESE ACCOMPANYING GUIDELINES:

a) Internet facilities are provided by the Academy as a tool to enable staff to enhance their professional activities, including teaching, research, administration and management. The Academy monitors all internet usage.

b) All individual members of staff will have access to the Internet where this is appropriate to their professional activity or the education of students.

c) All authorised Internet users must be given a copy of this policy and return the signed Employee declaration (Appendix 1) confirming they have read and understand the policy and guidelines.

d) Cases where concerns are raised that staff are intentionally misusing the Academy's Internet facilities will be investigated and, if deemed appropriate, will be dealt with under the Academy's disciplinary procedure.

e) Staff must ensure, whenever practically possible, that the facility is not used by anyone who has not been given authorisation.

f) Staff are required to inform an appropriate manager if they become aware of, or suspect that the Academy's internet facilities are being misused.

g) Access should only be made via the authorised account and password, which must not be made available to any other person.

h) In all cases, Internet access must be arranged by the ICT Technical staff and appropriate virus control software must be in place. Such virus protection software must not be "turned off" by non-ICT staff as removing or disabling virus protection software could lead to disciplinary action being taken.

i) The Academy reserves the right to examine or delete any files that may be held on its devices or computers systems. All Internet usage is monitored.

2. INTRODUCTION

2.1 The Policy on the use of the Internet and these guidelines have been produced to ensure that Academy employees are fully aware of the rules concerning the use of the Internet and the actions that could result should any misuse be detected.

2.2 The policy and guidelines deal with employees accessing data published by other organisations and available on the Internet.

2.3 The policy and guidelines cover use of the internet both within and beyond the Academy when the internet is accessed using Academy equipment, e.g. using an Academy laptop or by remotely accessing the Academy network; however it is not essential for staff to work at home.

3. SCOPE

3.1 The policy and guidelines apply to all employees of the Academy.

4. THE INTERNET

4.1 The Internet is a series of communication links, which enables computers around the world to access information and exchange files. The Internet allows users to obtain information held (and published) on computers anywhere in the world easily and relatively quickly. It also allows users to send information (such as orders) back to these computers. It is a huge freestanding network to which millions of users have access.

4.2 The legitimate business use of the Internet has increased beyond expectations in the last few years and there are no indications that this increase will not continue. Many organisations now make essential information available only via the Internet.

4.3 The open design of the Internet is its strength. However, the lack of controls and standards also exposes organisations (and private individuals) to an increased risk that networks and systems will be accessed improperly, data corrupted and viruses introduced.

5. AUTHORISED INTERNET USERS

5.1 All individual employees will be authorised to use the Academy's Internet facilities by signing the authorised as shown in Appenx 1. Copies of signed authorisation sheets will be retained by the Principal.

5.2 Under no circumstances should students access the internet using a staff log-in.

6. MISUSE OF THE ACADEMY'S INTERNET FACILITIES

6.1 Certain types of use of the Internet are unacceptable and they may also be illegal.

6.2 Cases where employees are suspected of intentionally misusing the Academy's Internet facilities, will be dealt with under the Academy's Disciplinary Procedure.

6.3 Examples of what is considered to be misuse of the Academy's Internet Facilities are given below, but this is not an exhaustive list:

7. ILLEGAL MATERIAL

The vast majority of information on the Internet is of a very interesting and informative nature. Unfortunately the Internet has also attracted the attention of many of the less desirable elements of modern society and information is available on the Internet, which is of an illegal, harmful, pornographic and obscene nature.

Unacceptable Material

7.1 It is illegal to create, access, copy, store, transmit or publish any material, which falls into the following categories:

National Security - Instructions on bomb making, illegal drug production, and terrorist activities;
Protection of Minors - Abusive forms of marketing, violence, and pornography;
Protection of Human Dignity - Incitement to racial hatred or racial discrimination. harassment;
Economic Security - Fraud, instructions on pirating credit cards;
Information Security - Malicious hacking;
Protection of Privacy - Unauthorised communication of personal data, electronic harassment;
Protection of Reputation - Libel, unlawful comparative advertising;
Intellectual Property - Unauthorised distribution of copyrighted works e.g. software or music.

Unacceptable Activity

7.2 It is unacceptable to create, access, copy, store, transmit or publish any material which is:

- Obscene, Vulgar.
- Likely to irritate or waste time of others.
- Subversive to the purposes of the Academy.
- Damaged to the reputation of the Academy.

For the purposes of these guidelines, obscene and vulgar are defined as follows:

- Obscene - Indecent, Lewd, Repulsive.
- Vulgar - Offending, Against good taste, Coarse.

When assessing whether material is unacceptable, each case will be judged on its merits, taking into account the individual circumstances.

Private Use

7.3 The use of the Academy's Internet or email facilities is not permitted for the pursuit of a private business, or for personal financial gain or gambling.

7.3.1 Limited private use of the Academy's Internet facilities is permitted. When you are using the Internet and/or email at work for private use, you are still identifiable as an employee of Bricknell Primary School. You should not therefore engage in any activities that could bring Bricknell Primary School into disrepute. Personal use of the system, for browsing the Internet or sending external email messages to friends or family, should be moderator and in your own time. Private use should not interfere with your work.

7.3.2 When sending personal emails whilst using Academy ICT devices you must use a private email account not your name@Bricknell.hull.sch.uk.

7.3.3 All Internet use is monitored.

7.4 It is also unacceptable to undertake any activity, which is intended to:

- Corrupt any information held or transmitted on the Internet.
- Detect weaknesses in the security infrastructure (testing firewalls, cracking passwords)
- Disrupt the normal functioning of the Internet or related services (overloading transactions, introducing viruses)
- Damage the reputation of the Academy.

8. DOWNLOADING SOFTWARE

8.1 No software should be downloaded on to the Academy network nor onto Academy equipment unless that download is carried out by RM Technical Staff.

8.2 Staff should:

- Not post information and photos about themselves, or Academy-related matters, publicly that they wouldn't want employers, colleagues, students or parents to see.
- Keep passwords secret and protect access to accounts.
- Not befriend students on social networking sites.
- Keep personal phone numbers private and not use their own mobile phones to contact pupils or parents.
- Use an Academy mobile phone when on an Academy trip.
- Keep phones secure while on Academy premises and report thefts to the police and mobile operator as soon as possible.
- Ensure that Academy rules regarding the use of technologies are consistently enforced.
- Not personally retaliate to any incident.
- Report any incident to the appropriate member of staff in a timely manner.

9. REVIEW PROCESS

9.1 The policy and guidelines will be regularly reviewed to ensure that they remain timely and relevant.

By clicking accept, you agree to the rules laid out in this Acceptable Use Policy and are aware of the repercussions that could take place if broken.

Appendix 2

Bricknell Primary School
Acceptable Use Policy - Students

The School Policy

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users.

For my own personal safety:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications.
- I will ensure I keep my Username and Password safe – I will not share it, nor will I try to use any other person's username and password.
- I will be aware of "stranger danger", when I am communicating on-line.
- I will not disclose or share personal information about myself or others when on-line.
- If I arrange to meet people off-line that I have communicated with on-line, I will do so in a public place and take an adult with me.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

I understand that everyone has equal rights to use technology as a resource and:

- I understand that the school ICT systems are primarily intended for educational use and that I will not use the systems for personal or recreational use unless I have permission to do so.
- 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 use the school ICT systems for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (eg YouTube), unless I have permission of a member of staff to do so.

I will act as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.

I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the school:

- I will only use my personal hand held / external devices (mobile phones / USB devices etc) in school if I have permission. I understand that, if I do use my own devices in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I 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 immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any attachments to emails, unless I know and trust the person / organisation who sent the email, due to the risk of the attachment containing viruses or other harmful programmes.
- 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.
- I understand the use of Social Media and Chats site is prohibited in school and I will not use these types of media.

When using the internet for research or recreation, I recognise that:

- I should 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 try to download copies (including music and videos)
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

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

- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action. This may include loss of access to the school network / internet, detentions, suspensions, contact with parents and in the event of illegal activities involvement of the police.

By clicking accept, you agree to the rules laid out in this Acceptable Use Policy and are aware of the repercussions that could take place if broken.