BRIGSTOCK LATHAM'S SCHOOL

Online Safety Policy

Forward thinking and creative; valuing faith, tradition, community and achievement.

Introduction

ICT and the internet have become integral to teaching and learning within schools; providing children, young people, and staff with opportunities to improve understanding, access online resources and communicate with the world all at the touch of a button. At present, the internet based technologies used extensively by young people in both home and school include:

- Websites
- Social media
- Web enabled mobile/smart phones
- Online gaming
- Learning platforms and Virtual Learning Environments
- Blogs and Wikis
- Email, Instant messaging and Chat rooms
- iPads/Tablets
- Coding software
- Downloading music
- Skype, video broadcasting
- Apple/Windows/Android aps

Whilst this technology has many benefits for our school community, we recognise that clear procedures for appropriate use and education for staff and students about online behaviours, age restrictions and potential risks is crucial. These skills will be fundamental in the society our pupils will be entering.

Every effort will be made to safeguard against all risks, however it is likely that we will never be able to completely eliminate them. Any incidents that do arise will be dealt with quickly and according to policy to ensure that children, young people, and staff continue to be protected.

At Brigstock Latham's C of E Primary School we encourage pupils to use the rich information resources available on the Internet and to develop appropriate skills to analyse and evaluate such resources. Local Authority guidelines for Acceptable Use should be read in conjunction with this policy.

This policy provides support and guidance to parents/carers and the wider community (where appropriate) for the safe and responsible use of these technologies beyond the school or educational setting. It also explains procedures for any unacceptable use of these technologies by children or young people, and refers to school disciplinary procedures for staff.

Purpose

- To emphasise the need to educate governors, staff, children and young people about the pros and cons of using new technologies both within, and outside of, the school environment.
- To provide safeguards and rules for acceptable use to guide all users in their online experiences.
- To ensure adults are clear about procedures for misuse of any online technologies both within and beyond the school or educational setting.
- The purpose of Internet Access in school is to raise educational standards to support the professional work of the staff and to enhance the school's management information and business administration systems.
- Access to the Internet is necessary to staff and pupils both as a curriculum requirement and working tool.
- To emphasise the need to educate governors, staff, children and young people about the pros and cons of using new technologies both within, and outside of, the school environment.
- To provide safeguards and rules for acceptable use to guide all users in their online experiences.

Scope

This policy applies to all staff, pupils, governors, visitors and contractors accessing the internet or using technological devices on school premises. This includes staff or pupil use of personal devices, such as mobile phones or iPads which are brought onto school grounds. This policy is also applicable where staff or individuals have been provided with school issued devices for off-site use, such as school laptop, iPad, tablet or work mobile phone.

Responsibilities

All staff have a shared responsibility to ensure that children and young people are able to use the internet and related technologies appropriately and safely as part of the wider duty of care to which all who work in Brigstock Latham's C of E Primary School are bound.

We will use social networking sites responsibly and ensure neither our personal or professional reputation, nor the school reputation is compromised by inappropriate postings.

<u>Technical Staff</u>

The Head teacher/Computing subject leader is responsible for ensuring:

- That the school's ICT infrastructure is secure and not open to misuse or malicious attack.
- That anti-virus software is installed and regularly maintained on all school machines and portable devices e.g. staff laptops.
- That the school's filtering policy is applied and updated on a regular basis.

- That any problems or faults relating to filtering are reported to the Online Safety Lead who will in turn report them to the IT provider.
- That users may only access the school's network using a personal log in.
- That he/she keeps up to date with online safety technical information in order to maintain the security of the school network and safeguard children and young people.

Children and Young People

Children and young people are responsible for:

- Annually signing agreement to, and abiding by, the Acceptable use agreement. (Appendix 1)
- Using the internet and technologies in a safe and responsible manner within school.
- Informing staff of any inappropriate materials, cyberbullying or contact from unknown sources (age dependant).

Incident Reporting

In the event of misuse by staff or students, including use of the school network in an illegal, unsuitable or abusive manner, a report must be made to the Head teacher/Designated Safeguarding Lead Person immediately.

Monitoring

The Online safety lead will regularly monitor and record user activity.

The Curriculum

Pupil Access to the Internet

Electronic information research skills are now fundamental to preparation of citizens and future employees, during the information age. We use the internet as a learning tool within the curriculum. At Brigstock Latham's Primary School we strive to embed online safety in all areas of our curriculum and key online safeguarding messages are reinforced wherever ICT is used in learning.

Parents are informed of pupil use of electronic information resources. An adult will be responsible for the children whilst they are accessing the internet. Access to on-line resources will enable pupils to explore thousands of libraries, databases and bulletin boards whilst exchanging messages with people throughout the world. Pupils regularly receive guidance and awareness of e-safety issues.

Guidelines for Internet Use

- An adult must make regular checks when pupils are accessing the internet in school.
- All users are responsible for good behaviour whilst using the Internet.
- The Internet is provided to conduct research and communicate with others.
- Individual users of the Internet are responsible for their behaviour and communications over the network. Users must comply with school standards.

- During school, teachers will guide pupils towards appropriate materials. Outside of the school, families bear responsibility for such guidance.
- Passwords will be changed at regular intervals.

The following are not permitted:

1. Sending or displaying offensive messages or pictures
2. Using obscene language
3. Harassing, insulting or abusing others
4. Damaging computers or systems
5. Violating copyright laws

Violations of the above will result in a temporary or permanent ban on Internet use.

Staff and Volunteers' Internet Usage and Security

All staff and volunteers should be aware of the importance of computer and internet security, and keep all machines, their content and any software or encrypted memory sticks, secure and safe from unauthorised access. Staff should not install any non-approved software on school computers or school-owned laptops and must ensure they keep the anti-virus software updated.

Specific guidance

Email Use

- The school provides all staff with a professional email account to use for all school related business, including communications with children, parents and carers. This allows for email content to be monitored and protects staff from the risk of allegations, malicious emails or inappropriate contact with children and their families.
- Under no circumstances will staff members engage in any personal communications (i.e. via hotmail or Google accounts) with current or former students outside of authorised school systems.
- All emails should be professional in tone and checked carefully before sending, just as an official school letter would be.
- Staff should inform their line manager or the Head Teacher or Online Safety Lead if they receive an offensive or inappropriate email via the school system.
- It is the responsibility of each account holder to keep their password secure and to report any suspected breaches of password security to the Online Safety Lead. Account holders must never share their password with another user, or allow access to their email account without the express permission of the Head Teacher.
- Supply teachers will be assigned their own log in for registers.

Managing Access

As technology continues to develop at an exponential rate, schools and their staff are increasingly taking advantage of opportunities for off-site access to the school network and email using remote access facilities. For data security and safeguarding purposes, it is crucial that staff are aware of the following restrictions on use both on and off site:

- Only store sensitive data on an encrypted memory stick or on your personal secured area of the school network.

- Log-on IDs and passwords should be confidential and use information that cannot be easily guessed (e.g. date of birth, telephone number, number patterns) and should be regularly changed.
- For security purposes, network access information should not be written down or stored with the device in case of theft or unauthorised access.
- Do not allow other users to access the internet through your personal user name and password.
- Ensure that logged in computers are locked when you're not present.

Internet Access and Age Appropriate Filtering

All students are entitled to safe and secure internet access and schools have a duty to deliver this as part of the learning experience. The Head Teacher is ultimately responsible for ensuring that the school infrastructure and network is as safe and secure as is reasonably possible and that age appropriate internet filtering is in place to protect young users from inappropriate or harmful online content. To this end, the school has the following filtering measures in place:

- Filtering levels are managed and monitored on behalf of the school by our broadband supplier or technical support, allowing an authorised school staff member to allow or block access to site and manage user internet access.
- Age appropriate content filtering is in place across the school, ensuring that staff and pupils receive different levels of filtered internet access in line with user requirements (e.g. available with staff log in but blocked to students)
- All users have unique usernames and passwords to access the school network which ensures that they receive the appropriate level of filtering. In addition to the above, the following safeguards are also in place.
- Anti-virus and anti-spyware software is used on all network and standalone PCs or laptops and is updated on a regular basis.
- A firewall ensures that information about children and young people cannot be accessed by unauthorised users.
- Encryption codes on wireless systems prevent hacking and unauthorised access.
- Staff are required to preview any websites before use, including those which are recommended to students and parents for homework support.
- Staff and pupils will be encouraged to adopt safe and responsible behaviours in their personal use of blogs, wikis, social networking and other online publishing.
- Staff to complete the online safety incident log if issues arise in school, either as a teacher or regarding child use.

<u>Mobile/Smart Phones Student use:</u>

- Students are not permitted to bring mobile phones/devices onto school grounds unless express permission has been granted by the Head Teacher for exceptional circumstances (e.g. independent journey to and from school)
- Where mobile phones have been allowed in the above circumstances, the device will be turned off and locked away by a responsible adult at the start of the school day and returned to the student before their homeward journey.

<u>Staff use:</u>

Personal mobile phones are permitted on school grounds, and it is accepted staff and volunteers will have access to the school WiFi for external internet access. Permission is granted on the basis that access will only occur outside of lesson time and when there are no children present.

- It is the responsibility of the staff member to ensure that there is no illegal or inappropriate content stored on their device when brought onto school grounds.
- Personal mobile phones should never be used to contact children, young people or their families, nor should they be used to take videos or photographs of students (refer to Staff Code of Conduct).

Social Networking Sites

Social Media sites are used by the school as a means of broadcasting information to parents/carers. All parents are required to give their consent via the 'Parent/Guardian Social Media Consent Form' before a photo of their child will be posted online. If there is no permission given, the child will not have their photo taken. In the event of a group photograph (e.g. sports team), any child who does not have consent to have their photograph published will be blocked out before posting online.

Twitter

Brigstock Latham's C of E Primary's Twitter account has been set up for the purpose of broadcasting administrative messages, and promote school activities and achievements to parents and carers.

Facebook

Brigstock Latham's C of E Primary School Facebook account is managed by Staff. The page is designed to broadcast administrative message and promote school activities and achievements to parents and carers. The staff decide on and authorise administrators that are responsible for updating the page on a regular basis. The administrators will communicate in a positive, accurate, respectful and responsible manner. They will uphold and promote the values of the school vision statement at all times.

Policy due for review	September 2021
Signed on behalf of the Governors	
Date ratified	September 2019