



BREWSTER AVENUE INFANT AND NURSERY SCHOOL

ONLINE SAFETY POLICY

This policy was ratified by the Full Governing Body on: 5th June 2019

Date for review (this policy will be reviewed every two years): Summer 2021

Contents

Introduction	3
Roles and Responsibilities.....	3
Headteacher and Senior Leaders.....	3
Network Manager / Technical staff	3
Teaching and Support Staff.....	4
Parents / Carers.....	4
The curriculum	5
Staff training	5
Use of the internet	5
Use of digital and video images	6
Social Media and mobile phones	7
Social Media - Protecting Professional Identity	7
Staff and Governor Acceptable Use Agreement	9

Introduction

This policy applies to all members of the Brewster Avenue Infant and Nursery School community (including staff, students / pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school / academy digital technology systems, both in and out of the school.

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These 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. Everyone should have an entitlement to safe internet access at all times.

Roles and Responsibilities

Headteacher and Senior Leaders

- The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community.
- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- provides training and advice for staff
- liaises with the Local Authority
- liaises with school technical staff
- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments

Network Manager / Technical staff

The Network Manager / Technical Staff / Co-ordinator for ICT / Computing is responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets required online safety technical requirements
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed

- that they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- that the use of the network / internet / Learning Platform / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher for investigation / action / sanction
- that monitoring software / systems are implemented and updated as agreed in school policies

Teaching and Support Staff

Are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current school Online Safety Policy and practices
- they have read, understood and signed the Staff Acceptable Use Agreement
- they report any suspected misuse or problem to the Headteacher for investigation / action / sanction
- all digital communications with students / pupils / parents / carers should be on a professional level and only carried out using official school systems
- online safety issues are embedded in all aspects of the curriculum and other activities
- students understand and follow the Online Safety Policy and acceptable use policies

Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about national / local online safety campaigns / literature e.g. Internet Safety Day. Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website and on-line student / pupil records

The curriculum

The education of pupils in online safety / digital literacy is an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum.

- A planned online safety curriculum should be provided as part of Computing / PHSE / other lessons and should be regularly revisited (at least termly)
- Key online safety messages should be reinforced as part of a planned programme of assemblies

Staff training

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- Annual online safety training will be delivered to staff as part of annual safeguarding training. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the schools Online Safety Policy and Acceptable Use Agreements.

Use of the internet

Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils. 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 systems. Internet access is an entitlement for students who show a responsible and mature approach to its use.

Internet access in the school is provided via a broadband link through an education specific provider E2BN. Filtering appropriate to the age of the pupils and appropriate virus protection is installed. Internet use is monitored and Wi-Fi access to the school's broadband service is protected by password.

The school will take all reasonable precautions to ensure that pupils only access appropriate material. However, due to the nature of internet content, it is not possible to guarantee that unsuitable material will never appear on a school device.

As part of the curriculum, pupils will be made aware of the guidelines for the acceptable use of the internet and what is not acceptable. All pupils will be given clear objectives when using the internet and will receive regular reminders on responsible use. Internet based activities will be planned to enrich learning. Curriculum activities that involve the use of the internet for gathering information and resources will develop pupils' skills in locating and evaluating material. Pupils will be taught how to judge the validity and likely accuracy of information found online. Where material gathered from the internet is used by pupils in their own work they will be taught to acknowledge the source of the information where appropriate.

The school will ensure that the use of internet materials by staff and pupils complies with copyright law.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular, they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Written permission from parents or carers will be obtained before photographs of students / pupils are published on the school website / social media / local press
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor

should parents / carers comment on any activities involving other *pupils* in the digital / video images.

- Staff are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that students / pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Photographs published on the website, or elsewhere that include students / pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.

Social Media and mobile phones

Children are not permitted to have mobile phones with them in school and the use of social media is not permitted by children in school.

Social media e.g. Twitter may be used where it is via the official school account and by authorised staff.

The use of mobile phones is not permitted when children are on site except in offices or the staff room. Mobile phones should be stored in lockers for the duration of the school day.

Social Media - Protecting Professional Identity

All schools, academies, MATs and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools/academies, MATs and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, engage in online bullying, discriminate on the grounds of sex, race or disability or who defame a third party may render the school or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through:

- Ensuring that personal information is not published

- Training is provided including: acceptable use; social media risks; checking of settings; data protection; reporting issues.

School staff should ensure that:

- No reference should be made in social media to pupils, parents / carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information



Staff and Governor Acceptable Use Agreement

This Acceptable Use Agreement is intended to ensure:

- that staff and governors 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 staff are protected from potential risk in their use of technology in their everyday work.

For my professional and personal safety:

- I will keep my username and password safe and secure – I will not share it, or 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 unpleasant, illegal, inappropriate or harmful material or incident, I become aware of, to the Headteacher.
- I will not disclose or share personal information about myself or others when online (this includes names, addresses, email addresses, telephone numbers, gender, age, educational or financial details).
- I will only communicate with pupils and parents/carers using official school systems. Any such communication will be professional in tone and manner. I will not contact pupils or parents/carers using personal email or phone (mobile or landline) unless urgent contact is required and for school business
- I understand that all my use of the school digital technology and communications systems can be monitored and logged and can be made available, on request, to the Headteacher.

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

- I understand that the school systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission.
- 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 systems or devices for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (eg YouTube), unless I have permission from SLT 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 own personal devices (mobile phones / USB devices etc) in school if I have permission. I understand that, if I do use my own devices in the *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 hyperlinks in emails or any attachments to emails, unless I know and trust the person / organisation who sent the email, 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 not install or attempt to install or store hardware or software of any type on any school device, nor will I try to alter computer settings, without permission.

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 will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory, and will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I understand that if I fail to comply with this Acceptable Use Agreement, I may be subject to disciplinary action.
- I will support and promote the school's Online Safety policy and help pupils to be safe and responsible in their use of ICT and related technologies.

Please sign to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement.

I understand this forms part of the terms and conditions set out in my contract of employment and that I am responsible for my actions in and out of the school. I agree to follow this Code of Conduct and to support the safe and secure use of digital technology throughout the school.

Signature _____ Date _____

Full name _____ (printed)