Highfield Community Primary School

E-Safety Policy 2023

Computing is an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, our school needs to build in the use of these technologies in order to support our young people to develop the skills to access life-long learning and employment.

Computing covers a wide range of resources including web-based and mobile learning as well as being a key tool for communication. It is important to recognise the constant and fast paced evolution of Computing within our society as a whole. Currently the internet technologies pupils are using both inside and outside of the classroom include:

- Websites
- Chat Rooms and Social Networking (such as Instagram, Facebook and Twitter)
- Coding
- Learning Platforms and Virtual Learning Environments
- Email and Instant Messaging
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile/Smart phones with text, video and/or web functionality
- Other mobile devices with web functionality

Whilst exciting and beneficial both in and out of the context of education, many computing resources, particularly those web-based, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies.

At Highfield Community Primary School we understand the responsibility to educate our pupils on eSafety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

The e-safety policy operates in conjunction with other policies and procedures including: Behaviour, Anti-Bullying, Safeguarding and Child Protection, Curriculum Policies, PSHE Curriculum, Data Protection, Mobile Phone, Security, Acceptable Use, Staff Handbook and Staff Code of Conduct.

E-Safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and pupils

- Sound implementation of e-safety policy in both administration and curriculum, including secure school network design and use.

- Safe and secure broadband.

- ICT support services will support Highfield Community Primary School with ICT problems and concerns.

The head teacher and governors have ultimate responsibility for the eSafety of all members of the school community. They ensure that the policy and practices are embedded and monitored.

eSafety skills development for staff

Our staff receive regular information and training on eSafety issues in the form of updates and inclusion within twilight and professional development programmes. New and trainee staff receive information on the school's acceptable use policy as part of their induction. All staff are made aware of individual responsibilities relating to the safeguarding of children within the context of eSafety and know what to do in the event of misuse of technology by any member of the school community.

Managing the school eSafety messages

We endeavour to embed eSafety messages across the curriculum whenever the internet and related technologies are used. The eSafety policy is introduced to pupils at the start of each school year and is a key part of our Computing and PSHE Curriculum. Relevant eSafety guidelines and SMART rules are prominently displayed throughout the school as part of our anti-bullying campaign. The children are reminded what to do if they see something that troubles or upsets them. The children understand they must then seek the help of the adult who has the responsibility of the class. As a school, we partake in Safer Internet Day activities annually in line with the national theme.

eSafety in the Curriculum

Computing and online resources are increasingly used across the curriculum. We believe it is essential for eSafety guidance to be given to pupils on a regular and meaningful basis. eSafety is embedded within our curriculum and we constantly seek new opportunities to promote eSafety to our children and families.

Educating pupils on the dangers of technologies that maybe encountered outside school is done informally when opportunities arise and as part of eSafety events. Pupils are aware of relevant legislation when using the internet such as data protection and intellectual property which may limit what they want to do but also serves to protect them. Pupils are taught about copyright and respecting other people's information, images, etc. through discussion, modelling and curriculum activities. Pupils are aware of the impact of online bullying and know how to seek help if they are affected by these issues. Pupils are aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/carer, teacher/trusted staff member, or organisations such as ChildLine and CEOP report abuse button.

Pupils have an understanding of the word permission and know that any work/images that are not their own, should not be posted on social media platforms without permission.

Data Security

The accessing and appropriate use of school data is something that the school takes very seriously. Staff are aware of their responsibilities when accessing school data. The level of access to school or student data is determined by the head teacher. Data can only be accessed and used on school computers or laptops. Any data which refers to sensitive information about pupils should not be openly transmitted across the internet via email – any such information should be password protected and/or initials are to be used to refer to individuals; personal information will only be shared using egress switch. All staff laptops and removeable storage devices are encrypted. SIMs is not available for staff to access outside of the school intranet. Staff and pupils are responsible for files stored in their personal space on school servers and any personal storage devices brought into school. There must be no use or distribution of malicious files.

Teaching and learning

Why Internet use is important

- The Internet is an essential element for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.

- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

- Pupils will use the Internet outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.

Internet use will enhance learning and benefit education:

- Access to world wide educational resources;

- Access to experts in many fields for pupils and staff;

- Professional development for staff through access to national developments, educational materials and effective curriculum practice;

- Collaboration across support services and professional associations;

- Improved access to technical support including the remote management of networks and automatic system updates;

- Exchange of curriculum and administration data;

- The school Internet access is designed for pupil use and includes filtering appropriate to the age of pupils;

- Internet access will be planned to enrich and extend learning activities;

- Pupils will be taught what Internet use is acceptable and what is not;

- Pupils will be educated in the effective use of the internet in research;

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

Managing Internet Access

The internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people. Highfield Community Primary School allows pupils, to have supervised access to internet resources through the school's fixed and mobile internet technology. Staff are recommended to preview any sites to be used with pupils prior to use. Raw image searches are discouraged when working with pupils; such sites are normally blocked for student use as part of the filtering service. If internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work. Parents will be advised to supervise any research.

All users are expected to observe software copyright and licensing terms at all times. It is illegal to copy or distribute software used within the school. Documents must not be published by users on the

internet which are defamatory or which may be intimidating, hostile or offensive to others on the basis of sex, race, colour, religion, national origin, sexual orientation or disability. Similarly, users must not access material on the internet which may be objectionable on the above grounds as they would violate the terms of the signed Acceptable Use Agreement. All users are expected to observe copyright of materials from electronic resources.

Infrastucture

School internet access is controlled web filtering service. Highfield Community Primary School is aware of its responsibility when monitoring staff communication under current legislation and takes account of;

- Data Protection Act 1998
- TheTelecommunications (Lawful Business Practice)
- Interception of Communication Regulations 2000
- Regulation of Investigatory Powers Act 2000
- Human Rights Act 1998

Staff and pupils are aware that school based email and internet activity can be monitored and explored further if required. If staff or pupils discover an unsuitable site, the incident is reported immediately to the eSafety co-ordinator or technical staff. It is the responsibility of the school, by delegation to the network technician, to ensure that anti-virus protection is installed and kept up-to-date on all school machines. Pupils and staff using personal removable media are responsible for measures to protect against viruses, for example making sure that additional systems used have up-to date virus protection software. It is not the school's or network technician's responsibility to install or maintain virus protection on personal systems. The school anti-virus software is set to automatically check the contents of any personal storage media attached to the system. It will automatically quarantine any suspected virus or malware identified on the personal storage media. Pupils and staff are not permitted to download programs or files on school based technologies, nor should they use any software or hardware designed to subvert the integrity of the school network. Technical staff should be informed if there are any issues related to viruses or anti-virus software.

E-mail

- Pupils may only use approved messaging accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive messages.
- Pupils must not reveal personal details of themselves or others in e-communications, or arrange to meet anyone.
- E-communications sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- Emails containing information about pupils and staff can only be sent through a secure email system.

Personal Mobile Devices (Mobile Phones, Phone Communications, I pads etc)

- Use of personal mobile phones onsite by staff should be kept to a minimum and restricted to staff only areas. Mobile Phones can only be used by staff at break and lunchtimes when they are not on duty.

- Personal mobile devices must not be used to take images of children.

- Parents and visitors are not permitted to use mobile phones when they are in school and are asked to switch them off.

- The use of school authorised mobile phones by staff is detailed in the policy relating to the use of school mobile phones.

- Pupils are not allowed to use mobile phones in school. Pupils in Y5 and Y6 who walk home by themselves are allowed to bring mobile phones into school but these must be given – switched off - to the teacher, who will store them securely until the end of the day.

- When leaving messages with external organisations or parents, staff are required to leave their full name and post. Where possible a direct contact number or extension number should also be given.

- The sending of inappropriate text messages between any member of the school community is not allowed.

- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

Published content and the school website

- The contact details on the Web site should be the school address, e-mail and telephone number.

- Pupil personal information will not be published.

- The Computing coordinator and school staff will take overall editorial responsibility and ensure that published content is accurate and appropriate.

- Computing coordinator will ensure that parents and pupils trying to publish comments to the school website are thoroughly checked before available for public viewing.

- Staff personal contact information will not be published. The contact details given online will be the school office and school contact details of selected key personnel only.

Safe Use of Images

Taking of Images and Movies

Digital images are easy to capture, reproduce, transform and publish and, therefore are easy to misuse. It is not appropriate to take or store images of any member of the school community or public, without having first sought consent and considered the appropriateness of such images. Our school records and SIMs contain an up-to-date record of parental/carer permission for the taking of images of our pupils. This record should be checked prior to taking images and in particular prior to publication of any images taken. With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment.

Pupils are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of others, this includes when on field trips and on school grounds at the end of the day, once the phone has been collected from the school office.

Publishing pupil's images and work

On a child's entry to the school, all parents/carers will be asked to give permission to use their child's work/photos in the following ways:

- on the school web site and Facebook page and in display material that may be used in external areas, i.e. local exhibitions

- in display material that may be used in the school's communal areas

- in the school prospectus, in printed publications for promotional purposes and in the local and national press

- Parents will also be asked to agree that when they take photographs when visiting school for an assembly, production etc. the photos that they take are for personal use and will not be posted on social media.

- This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue, e.g. divorce of parents, custody issues, etc. or an update to the school platform.

- Parents/carers may withdraw permission, in writing, at any time. Pupils' names (first name or full name) will not be published alongside their image and vice versa.

- E-mail and postal addresses of pupils will never be published.

- Photographs that include pupils will be selected carefully.

- Pupils' names will not be used anywhere on the school website particularly in association with photographs.

Social networking and personal publishing

- The school will block/filter access to social networking sites for pupil use. Teaching staff will have access to the school Facebook and Twitter page to keep updates current and relevant.

- Staff will follow acceptable use policy when uploading images to the school Facebook page and will ensure that consent list has been checked prior to publishing. All staff to have up to date list of children who do and do not have photograph permissions – for those children with permission, staff are aware of restrictions for certain platforms.

- Newsgroups will be blocked unless a specific use is approved.

- Pupils will be advised never to give out personal details of any kind which may identify them or their location.

- Pupils and parents will be advised of the dangers of the use of social network spaces outside school.

- Pupils and parents will be advised the use of social network spaces outside of school will remain the responsibility of the pupils and parents.

- Staff are strongly advised, in their own interests, to take steps to ensure that their personal data is not accessible to anybody who does not have permission to access it. All staff also need to be aware that parents and pupils may carry out web and social network service searches to find on-line information about staff, for example; background, interests, career experiences and

self-presentation. All staff, perhaps especially new staff in training and induction, are advised to ensure that information available publicly about them is accurate and appropriate.

- Staff must not use internet or web-based communication channels to send personal messages to a child/young person, or their parents. This includes online gaming.

- Staff should not have any secret social contact with children and young people or their parents, for example, using a pseudo name on a social networking site.

- Staff must not give their personal contact details to children or young people, including their parents.

- Staff are to understand that some of their communications may be called into question and may need to be justified.

- Staff must not have online communications with ex-students whom have recently left the school and may have friends or family still within the school.

- Staff are strongly advised to ensure that they enable all privacy and security settings on their social networking accounts, including the prevention of messages being sent to them as a result of an internet search. This will prevent young people accessing and potentially misusing their personal information, or making inappropriate contact.

- Staff must follow the school code of conduct when using social networking sites in their own time outside of work.

- When communicating with individual parents, staff will continue to use Marvellous Me.

ICT access

- All staff will be given the School e-Safety Policy and its importance explained.

- All staff must read and sign the 'Acceptable ICT Use Agreement' before using any school ICT resource.

- The school will keep an up to date record of all staff and pupils who are granted Internet access.

- Everyone will be made aware that Internet traffic can be monitored.

- Pupils will be informed that network and Internet use will be monitored in accordance with the student Acceptable Use Policy.

- Parents' attention will be drawn to the School e-Safety Policy in newsletters, the school brochure and on the school Website.

- Parents will be asked to sign and return the AUP.

- The school will take all reasonable precautions to ensure that users access only appropriate material. 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. Neither the school nor Gateshead Council can accept liability for the material accessed, or any consequences of Internet access.

- Complaints of Internet misuse will be dealt with by the Head Teacher.

- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the eSafety co-ordinator, depending on the seriousness of the offence; investigation by the head teacher/LA, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences .

Equal Opportunities

Pupils with additional needs

The school seeks to create a consistent message with parents for all pupils and this in turn aids the establishment and future development of the school's eSafety procedures and rules. Staff know that some pupils require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of eSafety issues. Where a student has poor social understanding, careful consideration is given to group interactions when raising awareness of eSafety. Internet activities are planned and managed to effectively support these pupils.

Assessing Risks

- Highfield Community Primary School will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor Gateshead Council can accept liability for the material accessed, or any consequences of Internet access.

- The school will regularly audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate