Beech Grove Primary School

Internet & E-Safety Policy 2023-2024

Introduction

The internet and other digital and information technologies are powerful tools which open up new opportunities for every one as part of everyday life. Beech Grove Primary School has a duty to provide pupils with safe, quality internet access as part of their learning experience.

Purpose

The internet is part of the statutory curriculum.

The purpose of internet use in school is

- to help raise educational standards
- to promote pupil achievement
- to support the professional work of staff and
- to enhance the school's management functions.

Pupils will also have access to the internet widely outside school and will, therefore, need to learn how to use and evaluate information wisely, being aware and recognising the need to take care of their safety and security when on-line.

E-Safety Policy

Beech Grove Primary School's e-safety policy has been written as part of a consultation process involving the Head Teacher, Senior Leadership Team and the Governing Body. It builds on advice from Government guidance.

The e-safety policy and its implementation will be reviewed annually. However, if new technology is introduced or incidents occur it may be reviewed more frequently.
The school's appointed e-safety co-ordinator is **Kerry Park**.

Adults and the E-Safety Policy

All members of staff, volunteers who work in school and parents will need to be aware of the e-safety policy and procedures.

Copies of the policy will be available on the school website, and from staff in the main reception.
Reference will also be made to the policy and procedures during events where e-safety may be highlighted, such as parents' consultations and parent information and demonstration sessions. (Ref section: Training)

Pupils and the E-Safety Policy

Safe and responsible use of the internet and technology will be reinforced across the curriculum with particular attention being given where pupils may be vulnerable or have special educational needs.

Pupils will be instructed in the responsible and safe use of the internet before having access to the internet in school and be made aware of what acceptable use is and what is not.
Pupils will then be guided to on-line activities that will support the learning outcomes planned for the pupil's age and maturity and access levels will be reviewed to reflect the curriculum requirements and age of pupils.
Staff will also ensure that pupils know how to keep themselves safe on-line and to ensure they have strategies to recognise when they may be in danger and be encouraged to report anything suspicious to a member of staff or on-line. (CEOPS)
Staff will provide regular e-safety training within a range of curriculum areas to increase pupil's on-line awareness.
E-safety rules will be posted in rooms with internet access to remind pupils of how to stay safe on-line.
There will be an additional focus on e-safety during the national e-safety week.

Access to the Internet & Learning Platform

The school will maintain a current record of all staff and pupils who are granted access to the school's electronic communications. All staff must read and sign the *Acceptable Use Policy* (AUP) before using any school Information Technology (IT) resource.

Parents will be informed that pupils will be provided with supervised internet access. They will be asked to share this information with their children and then sign and return a consent form for pupil access as part of the Home/School Agreement. At Key Stage 1 access to the internet will be by adult demonstration with occasional directly supervised access to specific approved on-line materials. At Key Stage 2 access to the internet will be supervised by members of staff at all times.
Only members of the current pupil and staff will have access to the school network.
All staff and pupils will be advised on acceptable conduct and use when using the school network. Its use by pupils and staff will be monitored by the Senior Leadership Team, Computing subject leader and staff regularly, in particular the message and communication tools and publishing facilities.
All users will be informed and regularly reminded of copyright issues and will only save appropriate content onto the school network.

Access to other Technologies and Devices

The school is responsible for ensuring all equipment is protected. As well as encrypting devices, training for staff should be provided to state how equipment should be transported and stored when off site – especially if it contains personal or confidential information.

Laptops

Staff will be made aware, in the AUP, that they are responsible for safeguarding school IT equipment for use in school and at home and pupil laptops for use in school.
Staff should take all precautions necessary to prevent theft, loss or damage of such items and prevent unauthorised access.

Removal of mobile technology from school premises is only permitted with prior authorisation from the Head Teacher and the equipment taken logged. Any equipment taken is for school use only.
On educational visits, school cameras and iPads may be taken off the school site for photography use only.

Mobile Phones

Staff are not permitted to use mobile phones during lesson times, unless prior consent is given from the Head Teacher. Staff can use their mobile phones on designated break times away from the children.

Children are not permitted to bring personal mobile devices into school, unless prior authorisation by the Head Teacher is gained. Any unauthorised devices, such as mobile phones, will be taken from the child and stored in a secure location until the end of the day. The child's parents/carers will be informed.

Training

The training needs of all staff will be audited annually through appraisal and discussions to ensure current awareness of resources available for both safety issues and learning. Liaising with the CPD Co-ordinator a training programme will be implemented for individual staff, year groups and, where necessary, the whole school. Training will then be monitored for its impact on teaching and learning.

Parents will also be kept informed on an annual basis about e-safety issues through the website, school newsletters and at events organised for parents, such as concerts and assemblies.

Security of Information Systems

The security of Beech Grove Primary School's information systems and users will be reviewed regularly. All servers, wireless systems, network components and cabling are securely located and physical access is restricted. Virus protection is installed on all school computers, laptops and iPads and configured to receive regular updates. Files held on the school's network will be regularly checked for viruses, Malware and Spyware. Software, including browser tool bars, will not be installed on school computers, laptops and iPads without prior consent from the Headteacher. An up-to-date record of all appropriate licences for all software is kept within school. The Computing Subject Leader and One IT, the technical support provider for Beech Grove, will review system capacity regularly and report any concerns to the Headteacher and SLT.

The school has agreed procedures for starters and leavers. A log is kept to identify which members of staff IT equipment has been assigned to, and members of staff are asked to sign for laptops for home use. Staff will be required to follow the agreed format for creating passwords (e.g. minimum of six characters in length, one upper case letter and a number to a maximum of sixteen characters), and the need to keep passwords secure. The Computing subject Leader will ensure that the IT technical support team is informed promptly of any member of staff/pupil joining or leaving the school. With regards to leavers, the IT support team will be asked to disable/remove user accounts.

Personal/sensitive data sent over the Internet or taken off site will be encrypted e.g. via password protected documents, encrypted portable storage devices and encrypted laptops. Portable media may not be used by staff without specific permission and will need to be virus checked prior to use on school devices.

Filtering

The school will ensure that the infrastructure/network are as safe and secure as possible. The filtering system is supplied by One IT. The filtering system offers a high level of protection that meets Internet Watch Foundation (IWF) standards. However the nature of the Internet makes it impossible to ensure that all inappropriate material is blocked.

The school will work with the LA and technical support provider to ensure that systems to protect pupils are reviewed and improved. Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable. Any material that the school believes is illegal will be reported to appropriate agencies such as IWF or CEOP. A flow chart to assist in how this can be done is available on the school area of the council website. If staff or pupils discover unsuitable content when using the internet/email, the URL/email must be reported to the schools e–Safety Co-ordinator who will follow the agreed school procedures. If the firewall identifies that any young person or staff member is using school IT facilities to engage in any searches or activities online which suggest a safeguarding or criminal act, they will be referred to the appropriate authorities, including Local Authority Safeguarding Team and local police.

The school's access strategy will be designed by teaching staff to suit the age and curriculum requirements of the pupils, with advice from network managers/ technical support providers.
Children will always be supervised by a member of staff when using IT equipment in school. Pupils' use of hardware is registered, and a log of registers are kept on the network to allow for investigation if needed.

Remote Access

When using any type of remote access to school data, members of staff are required to adhere to the school agreed password policy. All staff will sign an AUP regarding access to schools data. Third parties will only be given remote access with prior authorisation from the Headteacher and governing body.

Protection of Personal Data

Personal/sensitive data will be recorded, processed, transferred and made available according to the Data Protection Act 1998. Under the Data Protect Act (1998) all schools must comply with the eight enforceable principles of good practice. Data must be: Fairly and lawfully processed, Processed for limited purposes, Adequate, Relevant and not excessive, Accurate, Not kept longer than necessary, Processed in accordance with the data subject's rights, Secure and not transferred to other countries without adequate protection. All data should be kept secure and staff will be informed of what they can and cannot do with data.

Published Content

The school website will adhere to the statutory requirements as set out by the DfE and will comply with the school's guidelines for publications including respect for intellectual property rights and copyright. The Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate. The contact details on the website should be the school address, e-mail and telephone number. Staff or pupils' personal information must not be published.

Pupils' Images or Work

Images that include pupils will be selected carefully and will not provide material that could be reused. The school Image Consent Form ensures that all of the following points are covered:

Photographs, images and videos are regarded as personal data under the Data Protection Act (1998).

Photographs and videos will only be taken using school equipment and only for school purposes. Copyright, privacy and Intellectual Property Rights (IPR) legislation will be breached if images, video or sound are recorded without permission.

All staff/pupils are educated about the risks of taking, using, sharing, publishing and distributing digital media.

Written permission from parents/carers will be obtained before images of pupils are taken and published. Verbal consent must not be accepted under any circumstance. The same advice will apply to staff and the relevant consent obtained.

Staff are made aware that images of staff and/or pupils are not to be posted on third party websites (e.g. Facebook, Twitter, Instagram) as often the rights to the images transfer to the third party and may be sold on or distributed to advertisers without consent.

Pupils' full names will not be published (e.g. Websites and Newsletters) in association with photographs. If a photograph of an individual is used then it should not include the individual's name in the accompanying text or photo caption. If an individual is named in the text, then no photograph of that person will be included. If a group photograph is published then a general caption should be given e.g. school trip. If an individual supplies the school with a photograph, then it will not be automatically assumed that they are giving their consent to subsequent publishing.

The school will not reuse photographs after an individual appearing in them leaves the school. Any such photographs will be destroyed immediately or separate consent to continue to use the image for official purposes will be obtained.

Email

Email users within school are made aware, through training, that emails are covered by the Data Protection Act (1990) and the Freedom of Information Act (2000), meaning that safe practice should be followed in respect of record keeping and security. Staff are made aware that information stored on school or council equipment may be subject to release to the public at large under the Freedom of Information Act (FOI). Communications should be kept professional at all times. School Information stored on personal devices may also be subject to FOI.

Staff should only use school email accounts to communicate with pupils as approved by the Senior Leadership Team. Staff should not use personal email accounts during school hours or for professional purposes. All digital communications should be professional in tone and content. All emails sent from staff within school will have a standard disclaimer at the bottom stating that the email and any files transmitted within it may be confidential and are intended solely for the individual to whom it is addressed, and that any views or opinions are those of the author and not the school.

Access in school to external personal e-mail accounts is not permitted, as is the forwarding of chain messages. Staff and pupils are made aware, through the AUP, that all e-mail communications may be monitored.
Pupils may only use approved e-mail accounts (for example; gmail/live@edu/office 365). They must tell a teacher immediately if they receive offensive e-mail. Pupils must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission from an adult. Generic class email address should be used in primary schools for communication outside of the school to protect pupils' identities. E-mail sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.

Social networking, Social Media and Personal Publishing

The schools will block/filter access to social networking sites. Newsgroups will be blocked unless a specific use is approved.

As part of the Acceptable User Policy, staff are asked to ensure that any personal social networking sites, blogs, etc., that they create or actively contribute to, are not confused with their professional role. They are asked not to create, transmit, display, publish or forward any material that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or anything which could bring their professional role, the school, or the Council, into disrepute.

Staff are made aware that images of staff and/or pupils are not to be posted on third party websites (e.g. Facebook, Twitter, Instagram) as often the rights to the images transfer to the third party and may be sold on or distributed to advertisers without your consent.

Pupils will be advised never to give out personal details of any kind which may identify them and / or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and e-mail addresses, full names of friends, specific interests and clubs etc.

Pupils should be educated on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. They should be encouraged to invite known friends only and deny access to others. They should also be educated not to place personal photos on any social network space. Pupils should be encouraged to consider how public the information is and consider using private areas. Advice should be given regarding background detail in a photograph which could identify the student or his/her location eg. house number, street name or school. Pupils should be advised not to publish specific and detailed private thoughts.

Video-Conferencing

Equipment and network

All videoconferencing equipment in the classroom must be switched off when not in use and not set to auto answer. The equipment must be secure and if necessary locked away when not in use. Videoconferencing contact information should not be put on the school Website. Under no circumstances should school videoconferencing equipment should not be taken off school premises without permission.

Users

Parents and carers must agree for their children to take part in videoconferences. Only key administrators should be given access to the videoconferencing system, web or other remote control page available on larger systems. Unique log on and password details for the educational videoconferencing services should only be issued to members of staff and kept secure. Responsibility for the use of the videoconferencing equipment outside school time needs to be established with care.

Content

Approval from the Headteacher will be obtained in advance of the video conference taking place. All sessions should be logged including the date, time and the name of the external organisation/ person(s) taking part.

When recording a videoconference lesson, written permission should be given by all sites and participants. The reason for the recording must be given and the recording of videoconference should be clear to all parties at the start of the conference. Recorded material shall be stored securely. Copyright, privacy and Intellectual Property Rights (IPR) legislation will be breached if images, video or sound are recorded without permission.

Dialogue should be established with other conference participants before taking part in a videoconference. If it is a non-school site, the teacher should check that the participants are delivering material that is appropriate for the class. Videoconferencing should be supervised appropriately for the pupils' age and pupils using video conferencing equipment should be supervised at all times. All staff supervising video conferencing equipment should know the procedures to follow if they are unhappy with the content of a VC session e.g. how to 'stop' or 'hang up' the call.

E-safety Complaints

Any complaints of Internet misuse will be dealt with under the School's Complaints Procedure. The AUPs for staff and parents/pupils, will inform them of the complaints procedure. Any complaint about staff and pupil misuse must be referred to the Headteacher. Any issues (including sanctions) will be dealt with according to the school's disciplinary and child protection procedures. Discussions will be held with Middlesbrough Children's Safeguarding Board (MSCB) to establish procedures for handling potentially illegal issues for which the police will need to be involved.

All e–safety complaints and incidents will be recorded by the school — including any actions taken and kept for reference. Parents and pupils will be requested to work in partnership with staff to resolve issues.

Cyberbullying

Cyberbullying (along with all forms of bullying) will not be tolerated in school. Full details are set out in the school's policy on anti-bullying. There will be clear procedures in place to investigate incidents or allegations of cyberbullying, and all incidents of cyberbullying reported to the school will be recorded and kept as evidence. Pupils, staff and parents/carers will also be advised to keep a record of the bullying as evidence. Staff will be informed of procedures to follow in order to support any Beech Grove pupils affected by cyber bullying.