Bushfield Road Infant School

E-safety policy

Updated Autumn 2021

This policy will be reviewed annually, each autumn term, or earlier in the event of any updates.

Updates will be brought to the attention of all staff and governors at the earliest opportunity.

E-Safety Policy

The E-Safety policy has been written by the SLT, has been agreed by staff and approved by the governors. The policy will be reviewed on a yearly basis. All staff including teachers, supply staff, teaching assistants and support staff, will be provided with the E-Safety policy. All members of the school community have a duty to be aware of e-safety at all times, to know the required procedures and to act on them. The school's e-safety policy operates in conjunction with other policies including those for Safeguarding/Child Protection, Acceptable use and Anti-Bullying.

What is E-safety?

E-Safety is a safeguarding issue not an ICT issue. E-safety encompasses internet technologies and electronic communications, such as mobile phones and tablets as well as digital imaging and social networking. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience. It is the duty of the school to ensure that every child in its care is safe.

Why is Internet access important?

The Internet is an essential element in 21st century life. ICT skills and knowledge are vital to access life-long learning and employment, indeed ICT is now seen as a functional, essential life-skill along with English and Mathematics. The statutory curriculum requires pupils to learn how to locate, retrieve and exchange information using technology including the internet. All children should be taught to use the internet efficiently and safely, and to develop a responsible and mature approach to accessing and interpreting information. The internet provides many benefits to children and the professional work of staff, for example:

- Access to world-wide educational resources
- Access to experts in many fields
- Educational and cultural exchanges between children and young people worldwide
- Collaboration and communication within the wider context
- Access to learning wherever and whenever convenient.

The internet enhances the management information and business administration systems for example within:

- Communication systems;
- Improved access to technical support, including remote management of networks and automatic system updates;
- Online and real-time 'remote' training support;
- Secure data exchange between local and government bodies.

Managing access and the Internet safely

The purpose of internet access in schools is to raise educational standards, to support the professional work of staff and to enhance the school's management information and business administration systems. Access to the internet is a necessary tool for staff and entitlement for all pupils. It should be noted that the use of a computer system without permission for a purpose not agreed by the school could constitute a criminal offence under the Computer Misuse Act 1990.

Internet access will be planned to enrich and extend learning as an integrated aspect of the curriculum. Throughout the Foundation Stage, access to the internet will be by teacher or adult demonstration. Pupils will access teacher prepared materials rather than the open internet. At KS1, children will be taught how to use the Internet safely and effectively to carry out research. Whilst using the internet children and young people will be supervised at all times. An appropriate and approved filtering system is in place, which blocks harmful and inappropriate sites.

It is essential that children are safeguarded from potentially harmful and inappropriate online material. We ensure that children are taught about safeguarding, including online safety as part of a broad and balanced curriculum. This includes covering relevant issues through Relationships, Sex and Health Education.

The breadth of issues classified within online safety is considerable, but can be categorised into three areas of risk:

- content: being exposed to illegal, inappropriate or harmful material; for example pornography, fake news, racist or radical and extremist views;
- contact: being subjected to harmful online interaction with other users; for example commercial advertising as well as adults posing as children or young adults; and
- conduct: personal online behaviour that increases the likelihood of, or causes harm; for example making, sending and receiving explicit images, or online bullying.

All members of staff will sign an **Acceptable Use Policy** provided by 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.

Parents will be informed that pupils will be provided with supervised internet access, as well as opportunities to use other ICT technologies and will be asked to sign and return a permission form, as part of the e-safety acceptable use agreement.

Technical and Infrastructure

The school has an SLA with an ICT Service Provider, Adept (Doncaster) who are contracted one morning a week to manage the technical upkeep of the school's computer systems. Internet filtering and broadband provided by RM is in place to ensure that unsuitable/unsafe websites cannot be accessed by children. All systems have anti-virus, anti-spy ware and anti-spam ware software and firewalls installed, which are automatically updated to ensure that all networks remain up-to-date and safe.

In order to maintain the security of the systems, we:

- Maintain filtered broadband connectivity
- Work in partnership with the LA, Adept and RM to ensure any concerns about the system are communicated to the relevant officers so that systems remain robust and provide protection
- Ensure virus protection is installed on all appropriate hardware, and will be kept active and up to date
- Ensure the network is 'healthy' by weekly health checks on the network
- All staff will access computers using a unique, individually named user account and password for access to ICT equipment and information systems within school
- All staff have a responsibility for the security of their username and password. Users must not allow other users to access the systems using their log in details and must immediately report any suspicion or evidence that there has been a breach of security
- Users will be prompted to change their password at arranged intervals or at any time that they feel their password has been compromised

Education and Training

The school will take all reasonable precautions to ensure that users only access appropriate material. The sites used will be carefully selected for pupils by staff. The school will work with ACS, the LA and the internet service provider to ensure systems to protect pupils are reviewed and improved.

Children and staff must learn to recognise and avoid risks online and to become 'Internet Wise'.

- To STOP and THINK before they CLICK.
- To protect all personal information
- To consider the consequences their actions may have on others
- To discriminate between fact, fiction and opinion
- To search safely for internet content using age appropriate search engines/web sites
- To understand why on-line 'friends' may not be who they say they are and to understand why they should be careful in online environments
- To know what to do if they experience anything distressing, uncomfortable or threatening

Staff must also:

- Discuss, remind or raise any relevant e-safety messages routinely with pupils wherever suitable opportunities arise during all lessons.
- Provide a series of specific e-safety related lessons in every year group as part of the ICT curriculum
- Carefully plan any internet use to ensure that it is age appropriate and supports the learning objectives for specific curriculum areas.
- Ensure that when copying materials from the web, they understand issues around plagiarism: how to check copyright and also know that they must observe and respect copyright/intellectual rights.
- Ensure they know how to encrypt data where the sensitivity requires and that they understand data protection and general ICT security issues linked to their role and responsibilities e.g. CPOMS

Use of digital and video cameras

We gain parental/carer permission for use of digital photographs or videos involving their child as part of the school agreement when their son/daughter joins the school. Digital images/videos of pupils are stored in the teachers' shared images folder on the network and images are deleted at the end of the year. We will not use pupils' names when saving images in the file names. Photographs published on the School Website or in the local paper do not have children's names attached. We do not include the full names of pupils in the credits of any published school video materials/DVDs.

Parents may take photographs at school events: however, they must ensure that any images or videos taken involving children other than their own are for personal use and will not be published on the internet including social networking sites. All parents are verbally reminded of this before any school event.

As digital images (photographs and video clips) can now readily be taken using mobile phones, we have implemented a no mobile phone policy in school. Staff may only access their mobile phones at break and lunchtimes in the staffroom. Staff are not to use their mobile phone or personal camera to take photographs/video clips.

School Website

The Head teacher takes overall editorial responsibility to ensure that the school's ethos is reflected, the website content is accurate and the quality of presentation is maintained. Uploading of information is restricted to the SLT via the school's website management and maintenance provider (SeeGreen). The point of contact on the website is the school address and telephone number. The school website complies with the school's guidelines for publications. Parental permission is obtained to use photographs/videos of children on the school website. Any images published on the web do not have full names attached.

Social network and personal publishing

The school's filtering system blocks access to social/networking sites.

Both, children and staff need to understand how to ensure personal information is, and remains, private. Staff must not confuse or compromise their professional role with any online personal online activity, for example inviting children and young people into their personal social networking site.

Mobile phones, handheld devices and Smart watches

Mobile phones and personally owned devices will not be used in any way during lessons or formal school time. Mobile phone use is restricted to areas accessed by staff only. No images or videos should be taken on personal devices. Staff are not permitted to contact children or their families within or outside the setting in a professional capacity. Where staff members are required to use their mobile phone for school duties, for instance in case of a school emergency during off-site activities, or for contacting parents, they should hide (by dialling 141) their own mobile numbers for confidentiality purposes. Smart watches can be worn for work by members of staff. They are to be disconnected either by disabling notifications or switching on airplane mode. Mobile phones and personally owned mobile devices brought into school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personal devices.

How will complaints be handled?

Whenever a child or staff member infringes the e-Safety Policy, the final decision on the level of sanction will be at the discretion of the school management.

Staff

Category A infringements (Misconduct)

- Excessive use of internet for personal activities not related to professional development, e.g. online shopping, personal email, instant messaging, etc.
- Use of personal data storage media (e.g. USB memory sticks) without considering access and appropriateness of any files stored.
- Not implementing appropriate safeguarding procedures.
- Any behaviour on the World Wide Web that compromises the staff members' professional standing in the school and community.
- Misuse of first level data security, e.g. wrongful use of passwords.
- Breaching copyright or license e.g. installing unlicensed software on network.

Sanction – *referred to Head teacher*. Warning given.

Category B infringements (Gross Misconduct)

- Serious misuse of, or deliberate damage to, any school/Council computer hardware or software;
- Any deliberate attempt to breach data protection or computer security rules;
- Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent;
- Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988;
- Bringing the school name into disrepute.

Sanction – *referred to Head teacher/Governors/Local Authority Designated Officer and follow school disciplinary procedures*. Report to LA Personnel/Human resources, report to Police.

Other safeguarding actions due to infringement:

- The PC should be moved to a secure place to ensure that there is no further access to the PC or laptop.
- Instigate an audit of all ICT equipment by an outside agency, such as the schools ICT managed service providers – to ensure there is no risk of pupils accessing inappropriate materials in the school.
- Identify the precise details of the material.

If a member of staff commits an exceptionally serious act of gross misconduct they should be instantly suspended. Normally though, there will be an investigation before disciplinary action is taken for any alleged offence. As part of that the member of staff will be asked to explain their actions and these will be considered before any disciplinary action is taken. External support agencies are likely to be involved as part of these investigations.

In the case of images of child abuse being found, the member of staff should be immediately suspended and the Police should be called. The Local Authority Designated Officer (Stacey Darker) at the Child Protection Team should be informed.

How will staff and students be informed of these procedures?

- All staff will be required to sign the schools Acceptable use Policy record, which will be reviewed annually.
- Pupils will be taught about responsible and acceptable use and given strategies to deal with incidents so they can develop 'safe behaviours'.
- The school's e-safety policy will be made available and explained to parents, and parents will sign an acceptance form when their child starts school.
- Information on reporting abuse/bullying, etc will be made available by the school for pupils, staff and parents.
- Staff are issued with the 'What to do if?' guide on e-safety issues (Appendix 1)

This policy and The Acceptable Use Policy will be reviewed annually.
The Acceptable Use Policy record will be signed by all members of staff annually to agree that all possible and necessary measures to protect data and information systems will be taken. It will also confirm their responsibility for using the school's computer system in a professional, lawful and ethical manner.

Written: September 2021

To be reviewed: September 2022

Appendix 1

E-Safety Guidance
What to do if?

An inappropriate website is accessed unintentionally or intentionally by a child or member of staff:

1. Report it to the Head teacher and Designated Safeguarding Lead, Mrs T Bass or Deputy DSL, Mrs K Turnbull.
2. Notify the parents of the child.
3. Inform the school's IT Services provided by ACS and ensure the site is filtered.

An adult uses School IT equipment inappropriately:

The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to the appropriate authorities.

1. Ensure you have a colleague with you, do not view the misuse alone.

2. Report the misuse immediately to the head teacher, Mrs T Bass and ensure there is no further access to the PC or Laptop.

3. If the material is offensive but not illegal, the head teacher should then:
    - Remove the PC/Laptop to a secure place.
    - Instigate an audit of all IT equipment by the school's IT managed service providers to ensure there is no risk of pupils accessing inappropriate materials in the school.
    - Identify the precise details of the material.
    - Take appropriate disciplinary action (Contact Human Resources).
    - Inform Governors of the incident.

4. In an extreme case where the materials are of an illegal nature:
    - Contact the local police and follow their advice.
    - If requested, remove the PC/Laptop to a secure place and document what you have done.

If any bullying incident directed at a child occurs through e-mail or mobile phone technology, either inside or outside of school:

1. Advise the child not to respond to the message.
2. Secure and preserve any evidence.
3. Inform the Head teacher and designated safeguarding lead, Mrs T Bass.
4. Notify the parents of the children involved.
5. Inform the police if necessary.

If malicious or threatening comments are posted on social media about a pupil or member of staff:

1. Inform the Head teacher and designated safeguarding lead, Mrs T Bass and request the comment be removed.
2. Secure and preserve any evidence.
3. Inform the police as appropriate.

You are concerned that a child's safety is at risk because you suspect someone is using communication technologies (such as social networking sites) to make inappropriate contact with the child:

1. Inform the Head teacher and designated safeguarding lead, Mrs T Bass.
2. Inform the police and Children's services as appropriate.

Children should be confident in a no-blame culture when it comes to reporting inappropriate incidents involving the internet or mobile technology: they must be able to do so without fear.