BUSHFIELD ROAD INFANT SCHOOL

E-SAFETY POLICY 2017

E-Safety Policy

The E-Safety policy has been written by the ICT co-ordinator. The policy has been agreed by the Head teacher and 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, and its importance explained.

What is E-safety?

E-safety is not an ICT issue but a safeguarding issue. E-safety encompasses internet technologies and electronic communications, such as mobile phones 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. The school's e-safety policy operates in conjunction with other policies including those for Safeguarding/Child Protection, Acceptable use and Anti-Bullying.

Managing 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.

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.

Technical and Infrastructure

Schools IT are contracted to manage the technical upkeep of the school's computer systems. Internet filtering 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 to ensure any concerns about the system are communicated to the relevant officers so that systems remain robust and provide protection.
- Ensure the network is 'healthy' by annual health checks on the network.
- Never allow children or young people to access Internet logs.

Internet Policy and Procedures

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.

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.

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 the LEA 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 discriminate between fact, fiction and opinion
- To know some search engines/web sites that are more likely to bring effective results.
- 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.

Staff must also:

- 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.

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.

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 advised not to use their mobile phone or personal camera to take photographs/video clips without first gaining permission. If personal equipment is being used it should be registered with the school and a clear undertaking that photographs will be transferred to the school network and will not be stored at home or on memory sticks and used for any other purpose than school approved business.

School Website

The Head teacher takes overall editorial responsibility to ensure that the website content is accurate and the quality of presentation is maintained. Uploading of information is restricted to the administration officer. The point of contact on the web site is the school address and telephone number. The school web site 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.

How will infringements 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 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, 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.

This policy and The Acceptable use Policy will be reviewed annually.
The Acceptable 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.