BURTON MANOR PRIMARY SCHOOL

ONLINE SAFETY & ACCEPTABLE USE OF THE INTERNET POLICY

Approved: Spring 2018

Review: Spring 2019

Online-Safety & Acceptable Use of the Internet Policy Introduction

Pupils interact with new technologies such as mobile phones and the Internet on a daily basis and experience a wide range of opportunities, attitudes and situations. The exchange of ideas, social interaction and learning opportunities involved are greatly beneficial but can occasionally place young people in danger.
Schools must decide on the right balance between controlling access, setting rules and educating students for responsible use. Parents, libraries and youth clubs must develop complementary strategies to ensure safe, critical and responsible ICT use wherever the young people may be.

Online-safety covers issues relating to children and young people and their safe use of the Internet, mobile phones and other electronic communications technologies, both in and out of school. It includes education on risks and responsibilities and is part of the 'duty of care' which applies to everyone working with children. A new national e- safety drive is being led by the Child Exploitation and Online Protection Centre (CEOP) and detailed materials for schools are available from www.thinkuknow.co.uk)

What is the purpose of this policy?

This policy is intended to balance the desirability of fully exploiting the vast educational potential of resources for learning and communication with safeguards against the risks and unacceptable activity. It outlines the terms and establishes the ground rules by which the school provides access to the Internet and email, which must be accepted and adhered to by all users. It demonstrates the methods used to protect the children from sites containing unsuitable material. The benefits to pupils from access to the resources of the internet, far exceed the disadvantages. Ultimately, the responsibility for setting and conveying the standards that children are expected to follow, when using media and information resources, is one the school shares with parents and guardians. A combination of site-filtering, of supervision and by fostering a responsible attitude in our pupils promotes using the internet to enhance, consolidate and enrich learning.

The head teacher is the designated safeguarding officer.

To whom does the policy apply?

The policy applies to all users including:

- Governors
- senior managers
- teachers

- teaching assistants
- other adult members of staff
- community users
- parents
- pupils

Using the Internet to Support Teaching and Learning

The Internet offers great opportunities for teaching and learning. It can provide:

- A wider range of resources and materials which can enrich subject learning across a wide range of curriculum areas.
- opportunities to find up-to-date information and ask questions of experts via newsgroups;
- Opportunities for world-wide communication with other pupils and teachers;
- Opportunities for the development of independent learning and research skills;
- Access to global news as it happens and read newspapers from other countries;
- A range of support services;
- Virtual visits to places such as art galleries or places of worship;
- Development of network literacy (i.e. the capacity to use electronic networks to access resources, create resources and communicate with others - these can be seen as complex extensions of the traditional skills of reading, writing, speaking and listening, awareness of audience);
- Development of research and information handling skills.

What to be aware of

There is no overall control and there is no censorship of the Internet. Internet users must be aware that there is no defined standard for Internet publication and what is acceptable for some will be unacceptable for others. This may be due to standards of expression, language or tone in text or choice of images; cultural and social differences will mean that what is acceptable for one person, may not necessarily be acceptable for another.

Materials on the Internet vary hugely in quality: some materials are biased, inaccurate or misleading, either deliberately or unintentionally. For this reason Internet users need to be aware of the issues of quality and veracity, exercising caution and judgement in their use of any material they find. Anyone can publish material on the Internet – there is no guarantee that the information found is true or accurate, so children need to be encouraged to question what they find and verify it against other sources.

In addition, pupils need to be protected from obscene material and information relating to the misuse of drugs and the promotion of violence, intolerance, racism and extreme political and social views.

It is essential that Internet users understand the old stranger = danger messages in this context. Children should be told never to give any personal details on the Internet and they should be aware that people contacting them might not be who they claim to be. Issues, such as bullying by email, are emerging which schools also need to be concerned with.

The Internet is dynamic and material can be changed within seconds so you can never be sure that what you saw yesterday will be the same today - or even whether it will be there at all! New information is added on a daily basis and other information disappears.

There is also the potential for misuse of the technology. In recent years this has included pupils gaining unauthorised access to computer files and the irresponsible deletion of pupils' work on school networks which presents schools with organisational and management problems.

While educators and parents need to exercise caution in the Internet access allowed to pupils, we should not be deterred from using it. Its educational benefits outweigh any possible dangers. Schools have always helped learners to engage with society, based on clear support and guidance, and use of the Internet should be no exception.

As with television and video, parents, carers and educators should and where possible preview material or provide supervision, as well as having a more general strategy in place for ensuring children's safe use of the Internet.

What are the legal and ethical issues?

There are few legal precedents relating to the use of the Internet. There are a number of laws which are likely to apply to the use of the Internet in certain circumstances including the Obscenity Acts of 1959 and 1964, The Protection of Children Act 1978, The Indecent Displays Act 1981 and The Criminal Justice Act 1988. The use or modification of a computer system without permission or for a purpose not agreed by the school could constitute a criminal offence under the Computer Misuse Act 1990. In many cases, laws relating to copyright, libel, obscenity or incitement to racial hatred are likely to apply to the use of the Internet.

A school has a right and a duty to monitor the use of the Internet and email systems to prevent it being used for unlawful purposes or to distribute offensive material.
However, individuals have a right to privacy. Therefore, a school must balance the two separate rights. To comply with the first data protection principle of the Data Protection Act 1998 a school must be open on the subject of monitoring and establish a code giving guidelines on the use of email and the Internet and when individuals may use such systems for private communications.

Use of Information Systems

It is important to review the security of the whole system from user to Internet. This is a major responsibility that includes not only the delivery of essential learning services but also the personal safety of staff and pupils. ICT security is a complex matter and cannot be dealt with adequately in this document. The Schools ICT Security Policy provides further information regarding the information systems used in school.

The following measures are used:

- Children are expected to follow specific rules when using the Internet and e-mail. Misuse of the rules will result in direct action being taken.
- The security of the school information systems will be reviewed regularly.
- Virus protection will be updated regularly.
- Security strategies will be discussed with CFE or EIS.
- Personal data sent over the Internet will be encrypted or otherwise secured.
- Portable media may not used without specific permission followed by a virus check.
- Unapproved system utilities and executable files will not be allowed in pupils' work areas or attached to e-mail.
- Files held on the school's network will be regularly checked.

- The Computing subject Leader /SLT technician will review system capacity regularly.

Use of the Internet

We have taken the following measures to prevent children from Internet misuse and exposure to unsuitable materials:

- Staff and children are required to sign an Acceptable Internet and Email Use Agreement before access is granted

- Children are expected to follow specific rules when using the Internet and e-mail. Misuse of the rules will result in direct action being taken.

- Access to the Internet is gained via the school network. Children must have permission to use the Internet and must be supervised by an adult. Particular care must be taken when children are using free search engines.

- Images can be an excellent teaching tool. The Internet can provide a wonderful source of images, many of them copyright free, but finding appropriate images can be a challenge. Many major websites pre-set image searching from the homepage, often with safe searching options to filter results. However such searches and filters generally work on the basis of filename and description, and so can lead to misleading, unexpected or inappropriate results, sometimes of an adult nature. While teachers may find image searches useful in lesson preparation, they should always be used with care and caution, and are advised not to use them 'live' within a classroom setting.

- Staff check that sites pre-selected for pupils use are appropriate to need, age and maturity of pupils. Initially the pupils may be restricted to sites which have been reviewed and selected for content. As pupils gain experience, they will be taught how to use searching techniques to locate and specific information for themselves. We hope that pupils will learn to decide when it is appropriate to use the Internet, as opposed to other sources of information, in terms of: the time taken; the amount of information found; the usefulness and reliability of information located. Pupils will be encouraged to be critical users of the Internet; is the information true? How do you know? They will be encouraged to evaluate websites

- Computers are situated so that others can see what is on the screen.

- Staff are encouraged to take an interest in the Internet, to be aware of what research projects children are carrying out on the Internet and regularly discuss what young people see and use.

- Children are warned that there are unsuitable sites on the Internet and that people may try to contact them in an inappropriate way and the issues discussed.

- Policy Central software is used in school to ensure compliance with this policy. The r Computing leader analyses the Policy Central information. Incidents or misuse which is flagged up is discussed with children, staff, etc. Appropriate action is taken. For serious incidents school will seek advice from the County Department.

- Pupils are educated to use the Internet in a sensible manner and take responsibility for the information they access whilst connected to the Internet.

- Pupils are made aware that the writer of an email or author of a web page may not be the person they say they are.

- Pupils are encouraged to tell a member of staff immediately should they encounter any material that makes them feel uncomfortable.

- Access levels will be reviewed as pupils' Internet use expands and their ability to retrieve information develops.

- The school uses virus scanning software which is designed to intercept any viruses in email attachments and files downloaded from the Internet. Virus scanning software is also installed on appropriate school equipment. Virus protection is updated regularly.

- A record of all staff and pupils who have Internet access is maintained.

- The Head teacher will ensure that the policy is implemented effectively. (The head teacher will need to give a copy to new members of staff, governors, community members, etc. They will need to follow the policy and sign agreements prior to using the internet.)

- The Internet and Email facilities are provided for school related work only. Private use is not permitted. This applies to computers in school and teacher laptops.

- The Internet and Email facilities may not be used for:

(a) Transmitting, retrieving or storing any communications of a discriminatory or harassing nature or materials that are offensive, obscene, pornographic or sexually explicit.

(b) Deliberately propagating viruses, etc.

(c) Attempting to disable, defeat or circumvent any system intended to protect the privacy or security of another user.

- Internet users must not use or transmit abusive, profane or offensive language on or through the network's Internet and Email systems. Failure to comply may result in disciplinary action being taken.

- Email users must never send abusive, sexist, racist or defamatory messages.

- To help prevent access to undesirable sites, access to the Internet will be filtered using educationally based software.

- In addition to undesirable sites, other web mail providers, chat and news groups outside of the schoolmaster domain will be blocked.

- Accessing unauthorised sites is not permitted.

- All usage of the Internet will be monitored, logged and retained.

- Email contents are monitored, any suspected misuse must be reported to school staff accordingly.

- No user may knowingly use the Internet and Email facilities to:

(a) download or distribute pirated software or data, or

(b) download, copy or transmit the works of others without their permission as this may infringe copyright.

Disclaimer: Whilst the above measures will help to protect children using the Internet, neither the school nor the Internet service provider (ISP) can guarantee complete safety from inappropriate materials.

Use of images/video

Children's photographs will be used in school materials and in materials for the school community. Pupils may be named. (examples include displays around the school, Burton manor News and School Prospectus)

Children's photographs may be used for media coverage. This would include celebrating successes, special school events, new reception class in September, or when children are present at local / national events e.g. Commonwealth Service, Westminster Abbey, welcoming celebrities. Children's names may be used.
Any photographs which may be published on the internet would only have the children's images taken from behind. No faces will be seen and no names used.

Photographs / videos may be taken at school events by parents or close relatives of children at the school on the understanding that they are for private retention and not for publication in any manner.
This will apply to all children unless parents have specifically requested in writing that they do not wish their child to be photographed in one or all of the above categories.

The school is aiming to provide opportunities for children and parents to enjoy and record this special time when their offspring are young whilst at the same time doing the best to keep our valuable young people safe.

Parents must be aware that the withdrawal of permission to have photographs taken may exclude their child from participating in some opportunities. For example, if children are invited out of school to witness events, which have any possibility of media coverage we would be unable to include these pupils.

Use of email

At Burton Manor Primary School, we use Outlook Express to send e-mails. In Years 1/2 e-mails have been received and sent in a whole class situation. In Years 3/4 the children complete a unit of work focused on this area of ICT. The children are taught how to use the package, Outlook Express, safely to send and receive e- mails.

To safeguard our pupils we take the necessary steps:

- Pupils are encouraged to report any unpleasant material or messages sent, the report will be confidential and would help to protect other pupils.
- Pupils will be encouraged to report any messages received from unknown users or spam.
- Attachments to emails should only be opened if they are from a recognised and trusted source.
- Administrative staff/teachers/governors use individual email addresses that clearly identify their name and school.
- All email sent outside the School domain are not responsible by school.

Published Content & the School Website

The purpose of our school website is to provide information for existing and new pupils and parents. It is also designed to promote the school to prospective ones.

It is the duty of the school to ensure that every child in their care is safe, and the same principles should apply to the virtual presence of a school as would be applied to its physical buildings. We will ensure that no individual child can be identified or contacted either via, or as a result of a visitor using, the school website. The following safety measures will be taken;

- Personal information and e-mail identities will not be used on the website. The only point of contact will be to the school i.e. phone number and school address/email address

- Pupil's full names will not be used in image filenames or Alt tags.

- Children will be encouraged to report the use of inappropriate images, or the inappropriate use of images to their teacher, who should then report this to the ICT Co-ordinator and Head teacher.

- If showcasing digital video work, children will not be referred to by name, character names rather than real names will be used when filming, or a sound effect used to 'bleep' names out of the web version.

- Names will not be used in credits, the video will just be referred to as a class project, for example 'This video was produced by some of the children in Class 4'.

- Parental permission will be obtained before publishing any video footage, photographs of pupils, or examples of their work, on the school website.

- Text written by pupils will always be reviewed before being published on the school website. The work should not include the full name of the pupil, or reveal other personal information, such as membership of after school clubs or any other details that could potentially identify them.

- School will ensure there is no infringement of copyright through any content published on the website

- Links to any external websites will be thoroughly checked before inclusion on the school website to ensure that the content is appropriate both to the school and for the intended audience. Links will be checked regularly, not only to ensure that they are still active, but that the content remains suitable too!

- Cyber squatting and typo squatting are recognised problems in the area of domain name registration. Cyber squatting is when companies or individuals register the domain names of legitimate companies or organisations, often in the hope of making quick financial gains by selling the domain name back to the company. Typo squatting, also referred to as 'typo piracy', is when misspellings of domain names are registered in order to poach potential visitors away, often to inappropriate websites. Although both of these issues are more likely to affect commercial companies, we should nevertheless be aware of them, and therefore will check our domain names periodically. If we find that either of these issues present a problem, legal advice will be sought through the LEA in the first instance.

- The Computing Subject Leader, Head teacher and the office are responsible for all content which appears on the school website. The Head teacher will be the main point of contact for any queries regarding the website and its content, and the site will be regularly monitored to ensure that safety guidelines are being adhered to.

- The school website can provide an excellent mechanism for sharing safety advice with parents and carers. Safety advice will be reiterated through the website.

- Some schools have experienced cases of bullies manipulating digital images of their victims. Misuse of digital images by pupils will be dealt with seriously and the following sanctions for breach of the policy will be applied.

Social Networking, Mobile & Gaming Devices

The children are not allowed to visit social networking sites. If this occurs then the head teacher will discuss with the parents of the child involved and action will be taken. Our filter systems generally block social network sites.

Social networking is discussed in KS2 online-safety assemblies/Safer Internet Day. The children are advised to:

- never give out personal details.
- not place personal photos on any social network space.
- consider how public the information is and consider using private areas.
- Set up passwords, deny access to unknown block unwanted communications.
- invite known friends only and deny access to others.
- Students should be advised not to publish specific and detailed private thoughts.
- Report any bullying which takes place through social networking.

The children are not allowed to bring mobile phones and gaming devices into school. If a device is found in school, the teacher will remove and store the device until the end of the day. The head teacher will be notified of this and appropriate action will be taken.

Emerging Technologies

Many emerging communications technologies offer the potential to develop new teaching and learning tools, including mobile communications, wide Internet access and multimedia. A risk assessment needs to be undertaken on each new technology and effective practice in classroom use developed. The safest approach is to deny access until a risk assessment has been completed and safety demonstrated.

Safeguarding

In order to make best use of the many educational and social benefits of new technologies, pupils need opportunities to use and explore the digital world, using multiple devices from multiple locations. It is now recognised that e-safety risks are posed more by behaviours and values than technology itself. Adults working in this area must therefore ensure that they establish safe and responsible online behaviours. This means working to local and national guidelines on acceptable user policies.

Communication between pupils and adults, by whatever method, should take place within clear and explicit professional boundaries. This includes the wider use of technology such as mobile phones text messaging, e-mails, digital cameras, videos, web-cams, websites and blogs. Adults should not share any personal information with a child or young person. They should not request, or respond to, any personal information from the child/young person, other than that which might be appropriate as part of their professional role. Adults should ensure that all communications are transparent and open to scrutiny.

Adults should also be circumspect in their communications with children so as to avoid any possible misinterpretation of their motives or any behaviour which could be construed as grooming. They should not give their personal contact details to pupils including e-mail, home or mobile telephone numbers, unless the need to do so is agreed with senior management and parents/carers. E-mail or text communications between an adult and a child/young person outside agreed protocols may lead to disciplinary and/or criminal investigations. This also includes communications through Internet web sites.

Internal e-mail systems should only be used in accordance with the school/service's policy.

Personal Data Protection Online-Safety and CEOP

The Data Protection Act 1998 ("the Act") gives individuals the right to know what information is held about them and it provides a framework to ensure that personal information is handled properly. It promotes openness in the use of personal information.

Under the Act every organisation that processes personal information (personal data) must notify the Information Commissioner's Office, unless they are exempt.

The Data Protection Act 1998 applies to anyone who handles or has access to information concerning individuals. Everyone in the workplace has a legal duty to protect the privacy of information relating to individuals. The Act sets standards (eight data protection principles), which must be satisfied when processing personal data (information that will identify a living individual). The Act also gives rights to the people the information is about i.e. subject access rights lets individuals find out what information is held about them.

The eight principles are that personal data must be:

- Processed fairly and lawfully
- Processed for specified purposes
- Adequate, relevant and not excessive
- Accurate and up-to-date
- Held no longer than is necessary
- Processed in line with individuals rights
- Kept secure
- Transferred only to other countries with suitable security measures.

Schools will already have information about their obligations under the Act, and this section is a reminder that all data from which people can be identified is protected.

Sanctions for breaches of the policy

Sanctions for deliberate misuse of computer systems will ultimately be decided by the Head teacher and will depend on the seriousness of the offence. Minor offences may result in a warning or a temporary ban. Parents or guardians will be involved in more serious cases and in extreme cases access may be withdrawn and the offender permanently excluded, or in the case of staff misuse, dismissed. In the case of very serious offences – for example, using the schools computers to gain unauthorized access to other computers outside the school, then it may be necessary to involve the police. At all times legal advice will be sought through the LEA.

Home/School Links

Internet safety advice will be posted on the school's website and a paper copy sent to parents periodically via parent newsletter.