Bramingham Primary School

ICT

and

Acceptable Use Policy (staff & pupils)

Reviewed: November, 2017

Review date: November, 2018

Adopted by: ***Governors Committee meeting on 21.11.17***

Scope

This document provides the acceptable standards for use of the Internet and email by all school employees and children.

Responsibilities

It is the responsibility of the Governing Body to both adopt and review this policy on an annual basis and to advise the Headteacher of any required changes. Advice will be taken from Luton Borough Council on required policy updates as and when appropriate.

It is the responsibility of the Headteacher to publicise and make this policy available to all current and future staff, and to ensure that the standards within it are both monitored and enforced and to advise the Governing Body of any serious breaches of the policy. New staff will be provided with this policy as part of their induction pack

It is the responsibility of both the Headteacher and the Governing Body to take corrective and disciplinary measures as necessary when a breach of these standards occurs and to contact and co-operate with police and other law enforcement agencies where a breach of these standards constitutes a criminal act.

Introduction

The use of technology is an integral part of the National Curriculum and is a key skill for everyday life. Computers, tablets, programmable robots, digital still and video cameras and audio recording equipment can be used to acquire, organise, store, manipulate, interpret, communicate and present information. Furthermore, children are now required (under the new Primary Curriculum) to develop an understanding of computer science, including knowledge of computer hardware and software and networks (including the internet). The curriculum also explicitly states that children must learn to use technology safely and respectfully. As such, Bramingham Primary School recognises that its children are entitled to quality hardware and software and a structured and progressive approach to the learning of the skills needed to enable them to use it effectively and safely.

The purpose of this ICT policy is to state how the school intends to make this provision.

Rationale

The school believes that technology:

- can give children access to a rich source of materials
- can present information in new ways which help children understand, assimilate and use it more readily
- can motivate and enthuse children
- can help children focus and concentrate
- offers potential for effective group working
- has the flexibility to meet the individual needs and abilities of each child
- prepares children for their ongoing learning and eventually for their life as adults

Aims

The school's aims are to:

- provide a relevant, challenging and enjoyable computing curriculum for or all children
- meet the requirements of the National Curriculum Programme of Study for computing
- use technology as a tool to enhance learning throughout the curriculum
- respond to new developments in technology appropriately

Organisation

The school believes that progress in computing is promoted through regular access and use of technology relevant to a task.

- New skills may be introduced to a class or group of children
- Practice of skills will occur at appropriate times while using technology to support work across the curriculum

Resources

The school is aware of the need to continually maintain, update and develop its ICT resources and to make progress towards a consistent, reliable ICT service. The current resources are as follows:

- All classrooms have a class computer with hardwired connection to the network and internet.
- All classrooms have either a Smartboard and ceiling-mounted projector or a Clevertouch interactive screen, connected to the classroom computer.
- Some classrooms have a Smart airliner wireless slate.
- All classrooms in Years 1 – 6 are equipped with visualisers for use in classes as and when required.
- The IT/reprographics room has two networked printers, which are also photocopiers. Both black and white and colour printing is available.
- Two trolleys of laptops are available for use by classes. A bank of netbooks is also available. These computers all have wireless connectivity and allow access to the school network and the internet.
- Two trolleys containing 16 iPads in each are also available for use by classes. As with laptops, these are connected to the internet.
- Eleven other laptops, all with wireless connectivity, are available for use by individual children with Special Educational Needs or disabilities (SEND).
- A range of software is available throughout the school, although online resources are used much more frequently - supporting all areas of the curriculum.
- Each class has its own digital camera.
- A set of Easispeak microphones is available for use by any class, group or individual, as required.
- Four Apple TVs are available for use in classrooms. These enable sharing of children's work as well as online or other resources or apps, viewed via a connected iPad.

Internet and filtering

Internet is provided by the London Grid for Learning (LGfL) in conjunction with Trustnet. Filtering is applied to act as an additional safeguard for children. The level of filtering is applied per device; all curriculum laptops and tablet devices which are used by children have the highest level of filtering. Staff laptops and classroom PCs have staff level filtering applied. School IT technical support personnel have access to the management of the filtering system.

Curriculum

- All aspects of the computing curriculum are planned into year group planning to ensure coverage of computer science, digital literacy and information technology.
- Children are taught skills which they are able to use in creative and innovative ways to enhance their learning across all subjects.

Equal Opportunities

All children, regardless of gender and ability, will have equal access to IT facilities and will have the opportunity to make the most of their own potential within this field. Where additional resources are required to enable individual access, every effort is made to ensure that these are provided: for example, larger keyboards, track-ball controls or switched access.

Staff Training

The computing coordinator will assess and address staff training needs as part of the annual development plan process or in response to individual needs and requests throughout the year

Individual teachers should attempt to continually develop their own skills and knowledge, identify their own needs and notify the coordinator.

Administrative Systems

The school administration system is part of the whole school network, which is now configured as a virtual network. The management information system currently used is SIMs, and FMS is used for financial management. Both of these are currently being used as hosted systems (hosted by Capita). All school staff, both office-based as well as teachers and teaching assistants, use Office 365 and have email accounts associated with this. Office staff forward relevant emails which are received in the school admin email account to appropriate staff email accounts as required.

After Hours and Community Use

The school is always keen to explore ways of allowing controlled out of hours use by children and the community. Use is already made of some computing facilities by the After-School Club.

Health and Safety

The school is aware of the Health and Safety issues involved in children's use of technology and follows the recommendations made by the local authority and other reputable bodies. The school will dispose of redundant ICT equipment responsibly by offering to charities or disposing of safely and appropriately.

Security

- All IT equipment is noted in the school inventory
- Any equipment taken off site should be signed out by completing the relevant form, held on file by the computing coordinator.
- Anti-virus software is installed and is regularly updated through an automated process.
- Use of IT will be in line with the school's 'Acceptable Use Policy'
- Parents will be made aware of the 'Acceptable Use policy' and will be asked to give signed permission for their children to use computers, the Internet and email in school (Appendix 2)
- All children and parents will be aware of the School Rules for Responsible Use of ICT and the Internet (Appendix 1) and will understand the consequence of any misuse.

Acceptable Use of the internet by children

Rationale

Computers and the use of the Internet are a valuable resource for learners of all ages. The school's ICT Policy sets out how the school intends to teach computing and use technology to benefit its children's education. However Bramingham Primary School acknowledges that computers and the internet do have the potential for inappropriate use and access to undesirable material and that we have a duty of care to protect our children.

The purpose of this policy is to set out the procedures by which the school will minimise the misuse of computers and associative technology.

General use of Computers

- The use of school computers by children will be permitted only for purposes directed by the school
- Users are not permitted to access and amend another user's work without permission
- All computers connected to the internet will be protected by anti-virus software which will be kept up to date to check for the latest viruses
- The school reserves the right to look at any files on their systems including text, graphics and emails
- The school reserves the right to deny access to school computer systems

Internet Access

- The school provides internet access for educational purposes and should only be used by staff, children and members of the community for these purposes
- The school connects to the internet via the filtered service provided through the local authority. Children cannot use computers without filtered access.
- Where reasonably possible, all internet access by children is supervised by a member of staff or other responsible adult
- No child, member of staff or community user is permitted to access material that is illegal or potentially offensive using school systems
- The copyright and intellectual property rights of material using the school system will be respected
- Parents will be asked to sign a contract indicating that they understand the issues and give consent for their child to use the internet. This contract will also outline that children are not expected to actively attempt to access or distribute unacceptable material on school systems

Use of email

- Children may be given email access at the discretion of the staff. Group email addresses will be used for many purposes.
- Any user of the school email system must not use the system to communicate offensive, suggestive or defamatory material.
- Email messages sent and received from school systems should not be considered private. Children and staff should be aware that emails could be inspected at any time.

Publishing on the Internet

The school has its own website. Material published on the website has public access. However, the website also includes password-protected areas which enable resources to be uploaded and made available only to designated people (eg. parents of children in a particular class, governors, or staff).

All staff responsibilities

Employees must adhere to these standards in the following circumstances:

- When working on school premises
- When using equipment and utilities (hardware, software or mail and internet access) provided by the School, the LA or Luton Borough Council at home or other locations

The standards apply regardless of whether access occurs during or outside contracted work hours. Employees must alert the Headteacher or a relevant senior member of staff where a breach of these standards is suspected or known to have occurred.

Email Use

Email, via Office 365, is provided for school business use. Content of emails sent using school email system should be substantially related to workplace matters.

Email should never be sent, forwarded or replied to where the content is adult, explicit offensive or otherwise inappropriate.

Internet Use

Access to the internet is similarly provided for school use. Sites and groups visited should be related to workplace matters in the main. Staff may use other internet sites outside of their contracted hours, so long as they do not contain any material which is deemed inappropriate in any way.

Conducting financial activities on the Internet

While this policy does not specifically ban the use of the internet for conducting personal financial transactions e.g. online banking, we warn against it. Residual information from such activities can be left on your computer hard drive and could subsequently be accessed by others. Neither the school, the LA nor the council accept any liability for any resulting loss or damage.

Passwords

All school staff have a username and password to access the school network. Staff should never disclose their network password to any other person. Staff should use their own network username to log on to the school network when they need to use it. Staff should log off their computer, or lock it, when not using it or when leaving the area.

Staff should not disclose passwords to any online services (including Office 365) to any other person.

Passwords chosen should be easily remembered but difficult to guess. A pass-phrase, rather than a password, may provide a higher level of protection.

Printed lists of children's passwords should be avoided wherever possible; if they are needed, they must be held securely, and never left in view of other children.

Data protection

Staff should be aware of their responsibilities with regard to data protection (full details available in the data protection policy). In particular, staff should exercise great care when holding any personal data on laptops or memory sticks which may be taken off the school premises. Most teaching staff should not need to retain confidential data on portable media. In cases where a member of staff (eg. Special Needs Coordinator) legitimately needs to carry confidential data off-site, encrypted memory media should be used where possible.

Use of mobile phones and cameras.

Staff should not, as a matter of course, use their own mobile phone or camera to take photographs of children. Only in exceptional circumstances may this rule be waived. In such situations, the photos taken must be transferred to a secure area of the school's network within 24 hours, and deleted from the member of staff's phone or camera.

Publishing photos of children

Photos of children may be uploaded to the school website following general permission from parents when their child first begins school. In such cases, the children's full names will not be shown.

Use of social networking sites

All school employees are reminded that everything posted online is public, even with the strictest privacy settings. Once something is online, it can be copied and redistributed. Therefore, assume that everything that is written is permanent and can be shared.

School employees are reminded that they should at all times:

- Have the highest standards of personal conduct (inside and outside of school).
- Ensure that their behaviour (inside and outside of school) does not compromise their position within the school.
- Ensure that their relationship with members of the community, via social media, does not compromise their position within the school.
- School employees must not communicate, (including accepting 'friend' requests) with any current pupils of the school, or from any other educational establishment, on social networking sites such as Facebook. This is applicable even if a school employee has permission from a pupil's parent/guardian. (This would not apply to school aged pupils that an individual employee is directly related to, e.g. their child, niece or nephew).

Unacceptable use of Social Networking Sites/Applications

Through social networking sites/applications, school employees **must not**:

- Disclose private and confidential information relating to pupils, parents, other school employees, their employment directly or the school.
- Write abusive comments regarding current/previous school employees, pupils or parents/guardians
- View or update their personal site (on Facebook, twitter etc) during the working day, unless on a designated break. (This includes via a work or personal mobile telephone and/or iPad).
- Access or share illegal material
- Publish any content, which may be deemed as defamation or discrimination
- Post any images of pupils from the school or any other previous education establishment where the employee has worked
- Set up and/or use an alias social networking account to circumvent the policy
- Breach any of the schools other policies and procedures such as the School's Code of Conduct, Bullying and Harassment Policy, Equal Opportunities Policy
- Use it as a forum for raising and escalating concerns regarding the school or the Council. (These concerns should be raised using the Whistle Blowing Procedure.)

Staff should keep their personal information private when using social networking tools and protect the personal information of others. This not only includes the obvious information, such as name, address, phone numbers and school name, but also less obvious details. Staff should use the privacy features provided on the social networking sites, by password-protecting profiles and permitting access only to their own genuine friends.

Consequences of breaching the standards laid out in this policy

Deliberate access to inappropriate web content may constitute misconduct or gross misconduct. The use of email or the internet for the preparation, commission or abetting of a criminal act will constitute gross misconduct.

Bramingham Primary School

Children's Rules for Responsible Use of ICT and the Internet

The school has installed computers and internet access to help our learning.

These rules will help keep everyone safe and help us to be fair to others.

General

- I will treat school ICT equipment with care and respect
- I will not alter any computer settings without permission and if I have any problems I will contact a member of staff immediately
- I will not go into other people's files without permission
- I will only use computers for school work, homework and with permission playtime entertainment

Internet

- I will ask permission from a school adult before using the internet
- I will tell a member of staff if I find any unpleasant material on a site
- I understand that school may check which sites I have visited

Email

- I will only email people I know or my teacher has approved
- The messages I send will be polite and responsible
- I will report any unpleasant material or messages sent to me

I understand that I must keep the above rules and that if I misuse the school ICT system, my access to it may be withdrawn

Signed_____ Date_____

Dear Parent,

Use of Internet by Children

To support learning opportunities within the school, your child/children will at appropriate times be given access to the internet as an information source, a communications tool and a publishing medium.

The internet is a major source of educationally useful material and the primary distribution medium for a wide range of organisations. The potential to learners, as well as teachers, is significant and will continue to grow.

There are well publicised concerns regarding access to material on the internet that would be unsuitable for school children. Whilst it is impossible to ensure that a child will not access such material, the school, in conjunction with the local authority, is taking all reasonable steps to minimise a child's access to unsuitable material. These include:

- Use of a filtered internet service to prevent access to internet sites with undesirable material
- The requirement that wherever possible, all internet access during school hours will be supervised by a member of staff or another responsible adult
- Education of children as to the potential legal consequences of accessing certain types of materials.

Attached to this letter is a copy of the school's Acceptable Use of ICT Policy which we would ask you to read and a copy of the school's Rules for Responsible Use of ICT and the Internet which we would ask you to read to and discuss with your child in a way you feel appropriate to their age and understanding.

The school's website is being developed and may include information about many aspects of school life. Within published guidelines the school may publish pictures or work relating to your child. Please indicate on the form below your willingness (or not) for any reference to your child to be included on the school's website.

Parental Consent Form - use of the internet

Child's Name:_____ Class: _____

As parent or legal guardian of the above child:

- I give my permission for my son/daughter to use computer systems to access the internet and email.
- I have read the attached letter and understand that the school will endeavour to take all reasonable steps to restrict access to unsuitable material on the internet.
- I have read the attached Acceptable Use Policy
- I have read the Rules for Responsible Use of ICT and the internet and have discussed them with my child
- I give permission for photos of my son/daughter to be published on the school's website (full names of children will not be shown alongside photos).

Signature of Parent/Guardian _____ Date_____

Legislation

By signing the school's Acceptable Use Policy, all staff are stating that they understand and will comply with all of the requirements of this policy and of the various relevant government directives, as listed below:

Computer Misuse Act 1990
This Act makes it an offence to:
- Erase or amend data or programs without authority;
- Obtain unauthorised access to a computer;
- "Eavesdrop" on a computer;
- Make unauthorised use of computer time or facilities;
- Maliciously corrupt or erase data or programs;
- Deny access to authorised users.

Data Protection Act 1998
This protects the rights and privacy of individual's data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Act states that person 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.
- Not transferred to other countries without adequate protection.

Freedom of Information Act 2000
The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures.

Communications Act 2003
Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Malicious Communications Act 1988
It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.

Regulation of Investigatory Powers Act 2000
It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to:
- Establish the facts;
- Ascertain compliance with regulatory or self-regulatory practices or procedures;
- Demonstrate standards, which are or ought to be achieved by persons using the system;
- Investigate or detect unauthorised use of the communications system;
- Prevent or detect crime or in the interests of national security;
- Ensure the effective operation of the system.
- Monitoring but not recording is also permissible in order to:

- Ascertain whether the communication is business or personal;
- Protect or support help line staff.
- The school reserves the right to monitor its systems and communications in line with its rights under this act.

Trade Marks Act 1994
This provides protection for Registered Trade Marks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trade Marks must not be used without permission. This can also arise from using a Mark that is confusingly similar to an existing Mark.

Copyright, Designs and Patents Act 1988
It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. YouTube).

Telecommunications Act 1984
It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

Criminal Justice & Public Order Act 1994
This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they:
- Use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or
- Display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

Racial and Religious Hatred Act 2006
This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Protection from Harrassment Act 1997
A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Protection of Children Act 1978
It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is a anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison

Sexual Offences Act 2003
The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

Public Order Act 1986
This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence. Children, Families and Education Directorate page 38 April 2007.

Obscene Publications Act 1959 and 1964
Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

Human Rights Act 1998
This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of "higher law", affecting all other laws. In the school context, human rights to be aware of include:

- The right to a fair trial
- The right to respect for private and family life, home and correspondence
- Freedom of thought, conscience and religion
- Freedom of expression
- Freedom of assembly
- Prohibition of discrimination
- The right to education

These rights are not absolute. The school is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.

The Education and Inspections Act 2006
Empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.

The Education and Inspections Act 2011
Extended the powers included in the 2006 Act and gave permission for Headteachers (and nominated staff) to search for electronic devices. It also provides powers to search for data on those devices and to delete data. (see template policy in these appendices and for DfE guidance - http://www.education.gov.uk/schools/pupilsupport/behaviour/behaviourpolicies/f0076897/screening-searching-and-confiscation

The Protection of Freedoms Act 2012
Requires schools to seek permission from a parent /carer to use Biometric systems

The School Information Regulations 2012
Requires schools to publish certain information on its website: http://www.education.gov.uk/schools/toolsandinitiatives/cuttingburdens/b0075738/reducing-bureaucracy/requirements/changestoschoolinformationregulations