Technology – Acceptable use Policy

Lead member of staff	Helen Williamson
Governor Committee	Finance
Chair of Committee	A Sutton
Date of publication	February 2015
Reviewed date	23 May 2019

Outline

ICT in its many forms – internet, email, mobile devices etc – are now part of our daily lives. It is our duty to ensure that they are used safely and responsibly. All staff at Billingshurst Primary School are aware of the following responsibilities:-

- **Networked resources, including internet access, are potentially available to children and to all teaching, non teaching and office staff in the school**

- **All users must follow the conditions in the policy**

  Any **child** who does not follow the guidelines may lose the right to use the networked resources and to access the Internet. Any breach of the conditions will also be considered a disciplinary matter.

- Any breach of the conditions of the policy by a **member of staff** may lead to withdrawal of the user's access and in some instances could lead to criminal prosecution. Any breach of the conditions will also be considered a disciplinary matter.

- All staff, governors and visitors understand that ICT includes a wide range of systems, including mobile phones, digital cameras, laptops and tablets.

- All staff, governors and visitors understand that it is a disciplinary offence to use the school ICT equipment for any purpose not permitted by its owner.

- No staff, governors or visitors will disclose any passwords provided to them by the school.

- All staff, governors or visitors understand that they are responsible for all activity carried out under their username.

- Staff, governors and visitors will not install any hardware or software on any school owned device without the Head's permission.

- All staff, governors and visitors understand that their use of the internet may be monitored and if anything untoward is uncovered, could be logged and used in line with any disciplinary procedures. This includes all school owned devices. If an E-safety incident should occur, staff will report it to the Safeguarding officer as soon as possible.

- All staff, governors and visitors will use the school's email or internet and any related technologies for uses permitted by the Head or Governing Body. If anyone is unsure about an intended use, they should speak to the Head beforehand.

- All staff, governors and visitors will ensure that data is kept secure and is used appropriately as authorised by the Head or Governing Body. All devices used outside the school are encrypted. No data should be stored or transported via an unsecured memory stick.

- Personal devices must only be used in the context of school business with the explicit permission of the Head. Personal mobile phones or digital cameras must NEVER be used for taking any photographs related to school business. Each class has an ipad specifically for this purpose. These must never be used for personal use.

- All staff, governors and visitors using school equipment will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.

- All downloads must be removed from equipment outside of school when working via remote access or Office 365.

- All staff, governors and visitors will only use the approved email system and school email address for school business.

- Images will only be taken, stored and used for purposes within school unless there is parental permission for alternative use. When a child joins our school, parents are asked to sign if they agree to their child's images being used. If a parent does not agree to this, we ensure that their child's photograph is not used.

- Parents/legal guardians will sign to agree that any images they take at school events will be limited to personal/family use: they will agree not to upload these to social media sites.

- All staff, governors and visitors will make every effort to comply with copyright and intellectual property rights.

- All staff, governors and visitors will report any incidents of concern regarding staff use of technology and/or children's safety to the Head or the Deputy Designated Professional in line with our schools Safeguarding Policy.

- **Networked resources are intended for educational purposes** and may only be used for legal activities consistent with the rules of the school.

- Any expression of a personal view about the school or County Council matters in any electronic form of communication must be endorsed to that effect.

- All staff and governors understand that any communication sent by email could be subject to a Freedom of Information request and published.

- Any use of the network that would bring the name of the school or County into disrepute is not allowed.

- The school expects that staff will use new technologies as appropriate within the curriculum and that staff will provide guidance and instruction to children in the use of such resources.

- **Independent pupil use of the internet or the school's intranet** is not allowed. All access will be for educational purposes only and under adult direction and supervision.

- It is the teacher's responsibility that the internet facilities in the class room will be closed down at the end of each session [ie lunch time and end of school].

- Use of the internet by staff for private research is permitted outside school hours ie 7.30am – 8.45am and 3.30pm – 6pm.

Conditions for Use

- **Personal Responsibility**
  Access to the networked resources is a privilege, not a right. Users are responsible for their behaviour and communications. Staff and children will be expected to use the resources for the purposes for which they are made available. Users will accept personal responsibility for reporting any misuse of the network to the Headteacher.

  Acceptable Use
  Users are expected to utilise the network systems in a responsible manner. It is not possible to set hard and fast rules about what is and what is not acceptable but the following list provides some guidelines on the matter.

  Unacceptable Use
  a. Accessing or creating, transmitting, displaying or publishing any material [e.g. images, sounds or data] that is likely to cause offence, inconvenience or needless anxiety.

b. Accessing or creating, transmitting or publishing any defamatory material.
c. Receiving, sending or publishing material that violates copyright laws or Data Protection Acts.
d. Transmitting unsolicited material to other users [including those on other networks].
e. Unauthorised access to data and resources on the school network system or other systems.
f. User action that would cause corruption or destruction of other users' data, or violate the privacy of other users, or intentionally waste time or resources on the network or elsewhere.

Additional guidelines

a. Users must comply with the acceptable use policy of any other networks that they access.
b. Users must not download software without approval of the ICT co-ordinator.

Network Etiquette and Privacy

Users are expected to abide by the rules of network etiquette. These rules include but are not limited to, the following

a. **Be polite** – never send or encourage others to send abusive messages.
b. **Use appropriate language** – users should remember that they are representatives of the school on a global public system. Illegal activities of any kind are strictly forbidden. Do not use language that could be calculated to incite hatred against any ethnic, religious or other minority group.
c. **Privacy** - **do not reveal any personal information** [e.g. home address, telephone number] about yourself or other users. Do not trespass into other users' files or folders.
d. **Passwords** – **do not reveal your password to anyone.** If you think that someone has learned your password then contact the School Business Manager.
e. **Electronic Mail** - it is not guaranteed to be private. Messages relating to or in support of illegal activities will be reported to the authorities. Do not send anonymous messages. No names should be used in the headers of emails.
f. **Disruptions** – do not use the network in any way that would disrupt use of the network by others.
g. **Other Considerations** – be brief in your notes, cite references for any facts you present.
h. **Desks** – all desks must be left clear at the end of the day. No information containing personal or confidential data must be left unattended. All such files are locked away.
i. **Computers** – all computer screens must be locked when left unattended.

- **Services**

The school will not be responsible for anything which may inadvertently go wrong on the system eg working on a document, the system crashes and you lose the document.

- **Security**
  Users are expected to inform the Headteacher immediately a security problem is identified. Do not demonstrate the problem to other users. Users must login with their own user id and password, where applicable. Users identified as a security risk will be denied access to the internet.

- **Wilful Damage**
  Any malicious attempt to harm or destroy any equipment or data of another user or network connected to the school system will result in loss of access, disciplinary action and, if appropriate, legal referral. This includes the creation or uploading of computer viruses. The use of software from unauthorised sources is prohibited.

- **Media Publications**
  Named work and images of school children will not be published without written permission from parents/guardians being obtained. Named images of pupils will only be published once we have received written consent on the 'Consent Form for Photography and Images of Children'.

Parental Permission Form for Internet Access & Media / Electronic Release Form

As the parent / legal guardian of .....
I do / do not* give permission for my child to access networked computer services such as electronic mail and the Internet. I understand that children will be held accountable for their own actions. I also understand that although the school will take reasonable steps to ensure that my child is appropriately supervised, according to age and responsibility, I will not hold the school or County Council responsible for inappropriate material, which my child may obtain, despite such reasonable supervision. I accept responsibility for setting standards for my son/daughter to follow when selecting, sharing and exploring information and media. I agree to report any misuse of the network to the school.

* Please delete as appropriate

Name: (in print) _____

Signature: _____

Date: _____