Bishops Tawton Primary School

Acceptable Use Policy

Networked resources, including Internet access, are potentially available to students and staff in the school. All users are required to follow the conditions laid down in the policy.

Any breach of these conditions may lead to withdrawal of the user's access, monitoring and or retrospective investigation of the users use of services, and in some instances could lead to criminal prosecution. Any breach of the conditions will also be considered a disciplinary matter.

These 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. Any use of the network that would bring the name of the school or County Council 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 pupils in the use of such resources. All computer systems will be regularly monitored to ensure that they are being used in a responsible fashion.

CONDITIONS OF USE

Personal Responsibility

Access to the networked resources is a privilege, not a right. Users are responsible for their behaviour and communications. Staff and pupils will be expected to use the resources for the purposes for which they are made available. Users are to take due care with the physical security of hardware they are using. Users will accept personal responsibility for reporting any misuse of the network to a member of the SLT.

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:

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:

1. Be polite – never send or encourage others to send abusive messages.

2. 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.

3. Do not use language that could be calculated to incite hatred against any ethnic, religious or other minority group.

4. 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.

5. Password – do not reveal your password to anyone. If you think someone has learned your password then contact a member of the SLT.

6. Electronic mail – 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.

7. Disruptions – do not use the network in any way that would disrupt use of the network by others.

8. Pupils will not be allowed access to unsupervised and/or unauthorised chat rooms and should not attempt to gain access to them.

9. Staff or pupils finding unsuitable websites through the school network should report the web address to a member of the SLT.

10. **Do not attempt to visit websites that might be considered inappropriate.**

11. Files held on the school's network will be regularly checked by a member of the SLT.

12. It is the responsibility of the User (where appropriate) to take all reasonable steps to ensure compliance with the conditions set out in this Policy document, and to ensure that unacceptable use of the Internet/Intranet does not occur.

UNACCEPTABLE USE

Examples of unacceptable use include but are not limited to the following:

- Users must login with their own user ID and password, where applicable, and must not share this information with other users. They must also log off after their session has finished.

- Users finding machines logged on under other users username should log off the machine whether they intend to use it or not.

- 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. (The County Council have filters in place to block e-mails containing language that is or may be deemed to be offensive.)

- Accessing or creating, transmitting or publishing any defamatory material.

- Receiving, sending or publishing material that violates copyright law. This includes through Video Conferencing and Web Broadcasting.

- Receiving, sending or publishing material that violates Data Protection Act or breaching the security this act requires for personal data.

- Transmitting unsolicited material to other users (including those on other networks).
- Unauthorised access to data and resources on the school network system or other systems.

- 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.

- Cyberbullying

Additional guidelines

- Users must comply with the acceptable use policy of any other networks that they access.

- Users must not download software without approval from a member of the SLT.

SERVICES

There will be no warranties of any kind, whether expressed or implied, for the network service offered by the school. The school will not be responsible for any damages suffered while on the system. These damages include loss of data as a result of delays, non-deliveries, or service interruptions caused by the system or your errors or omissions. Use of any information obtained via the network is at your own risk.

NETWORK SECURITY

Users are expected to inform a member of the SLT immediately if a security problem I identified. Do not demonstrate this problem to other users. Users must login with their own user id and password, where applicable, and must not share this information with other users. Users identified as a security risk will be denied access to the network.

PHYSICAL SECURITY

Staff users are expected to ensure that portable ICT equipment such as laptops, digital still and video cameras are securely locked away when they are not being used.

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

Written permission from parents or carers will be obtained before photographs or videos of pupils are published. Named images of pupils will only be published with the separate written consent of their parents or carers.

Staff Communication with Children and Young People *(including the Use of Technology)*

Communication between children 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 children and young people 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 based web sites.

Internal e-mail systems should only be used in accordance with the organisation’s policy.

This means that the school should:

- have a communication policy which specifies acceptable and permissible modes of communication

This means that adults should:

- not give their personal contact details to children or young people, including their mobile telephone number and details of any blogs or personal websites
- only use equipment e.g. mobile phones, provided by organisation to communicate with children, making sure that parents have given permission for this form of communication to be used
- only make contact with children for professional reasons and in accordance with any organisation policy
- recognise that text messaging is rarely an appropriate response to a child in a crisis situation or at risk of harm. It should only be used as a last resort when other forms of communication are not possible
- not use internet or web-based communication channels to send personal messages to a child/young person
- ensure that if a social networking site is used, details are not shared with children and young people and privacy settings are set at maximum

Date: January 2014