WISBOROUGH GREEN PRIMARY SCHOOL

ACCEPTABLE USE POLICY

Reviewed Due Autumn 2017

Contents

Introduction

Networked Resources
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 user's 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 mane 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. Independent pupil use of the Internet or the school's Intranet will only be permitted upon receipt of signed permission and agreement forms as laid out below. 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. (See section 13.0 in the WSCC ICT in schools Acceptable Use Protocol guidance.) 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.

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 (eg 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 the ICT Technician.

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 students finding unsuitable websites through the school network should report the web address to the Headteacher.

10. Do not introduce memory or USB sticks into the network without having them checked for viruses.

11. Do not attempt to visit websites that might be considered inappropriate. (Such sites would include those relating to illegal activity.) All sites visited leave evidence in the county network if not on the computer. Downloading some material is illegal and the police or other authorities may be called to investigate such use.

12. Unapproved system utilities and executable files will not be allowed in pupils' work areas or attached to e-mail.

13. Files held on the school's network will be regularly checked by the school's ICT Technician.

14. 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:

1. Users must log in 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.

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

3. Accessing or creating, transmitting, displaying or publishing any material (eg 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.)

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

5. Receiving, sending or publishing material that violates copyright laws. This includes through Video Conferencing and Web Broadcasting (see section 8.0 in the WSCC ICT in schools Acceptable Use Protocol guidance.)

6. Receiving, sending or publishing material that violates the Data Protection Act or breaching the security this Act requires for personal data. (See section 9.0 respectively in the WSCC ICT in schools Acceptable Use Protocol guidance.)

7. Transmitting unsolicited material to other users (including those on other networks).

8. Unauthorised access to data and resources on the school network system or other systems.

9. 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

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

2. Users must not download software without approval from the IT manager.

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 any information obtained via the network is at your own risk.

Network Security

Users are expected to inform the Headteacher immediately a security problem is 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 I pads, laptops, digital still and video cameras are securely locked away when they are not being used. Items that need to be left over breaks and lunchtimes, for example, will need to by physically protected by locks and/or alarms.

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 of pupils are published. Named images of pupils will only be published with the separate written

consent of their parents or carers. (See section 12.0 for the standard Parent/Student Permission Form and the example Image Parent Consent Form).

Publishing includes, but is not limited to:

- The school website
- The Local Authority website
- Web broadcasting
- TV presentations
- Newspapers

Pupils' work will only be published (eg photographs, videos, TV presentations, web pages etc) if parental consent has been given.

Social Media

There are four key areas:
A. The use of social networking sites by pupils within school
B. Use of social networking by staff in a personal capacity
C. Comments posted by parents/carers
D. Dealing with incidents of online bullying

A. The use of social networking sites by pupils within school

Social networking sites should not be used/accessed in school unless under the direction of a teacher and for a purpose clearly apparent from the learning objective of the relevant learning experience. If social media sites are used then staff should carry out a risk assessment to determine which tools are appropriate. Social Media sites to be used in school include blogging sites (Primary blogger) and Twitter. Parents will give permission for children to access these sites in school as well as permission for images of their child / child's work to be included on the site. (See social Media consent form)

In terms of private use of social networking sites by a child it is generally understood that children under the age of 13 are not permitted to be registered, including Facebook and Instagram to name two.

B. Use of social networking by staff in a personal capacity

It is possible that a high proportion of staff will have their own social networking site accounts. It is important for them to protect their professional reputation by ensuring that they use their personal accounts in an appropriate manner.

Guidelines are issued to staff:

- Staff must **never** add pupils as 'friends' into their personal accounts (including past pupils under the age of 16).
- Staff are **strongly advised** not to add parents as 'friends' into their personal accounts.
- Staff **must not** post comments about the school, pupils, parents or colleagues including members of the Governing Body.
- Staff must not use social networking sites within lesson times (for personal use).
- Staff should only use social networking in a way that does not conflict with the current National Teacher's Standards.
- Staff should review and adjust their privacy settings to give them the appropriate level of privacy and confidentiality.
- Staff should read and comply with 'Guidance for Safer Working Practice for Adults who Work with Children and Young People'.
- Inappropriate use by staff should be referred to the Headteacher in the first instance and may lead to disciplinary action.

C. Comments posted by parents/carers

Parents and carers will be made aware of their responsibilities regarding their use of social networking. Methods of school communication include the prospectus, the website, newsletters, letters and verbal discussion. School policies and documents provide further information regarding appropriate channels of communication and means of resolving differences of opinion. Effective communication following principles of mutual respect is the best means of ensuring the best learning experiences for the child.

Parents must not post pictures of pupils, other than their own children, on social networking sites where these photographs have been taken at a school event.
Parents should make complaints through official school channels rather than posting them on social networking sites.
Parents should not post malicious or fictitious comments on social networking sites about any member of the school community.

D. Dealing with incidents of online bullying/inappropriate use of social networking sites

The school's Anti-Bullying Policy sets out the processes and sanctions regarding any type of bullying by a child on the school roll.

In the case of inappropriate use of social networking by parents, the Governing Body will contact the parent asking them to remove such comments and seek redress through the appropriate channels such as the Complaints Policy and will send a letter.

The Governing Body understands that, "There are circumstances in which police involvement is appropriate. These include where postings have a racist element or where violence is threatened or encouraged." Furthermore, "Laws of defamation and privacy still apply to the web and it is unlawful for statements to be written…which:

- expose (*an individual*) to hatred, ridicule or contempt
- cause (*an individual*) to be shunned or avoided
- lower (*an individual's*) standing in the estimation of right-thinking members of society or
- disparage (*an individual in their*) business, trade, office or profession." (National Association of Headteachers)

Documents to accompany this policy include:

- Staff User Form
- Pupil User Form
- User agreement and Parental Permission form for Internet access and Media/Electronic release form
- Parent permission letter for photographs

This policy is to be reviewed annually and amended as appropriate in light of national changes.