Holbrook Primary School

Acceptable Use of Technology Policy

Reviewed: Sept 2017 **By Daniel Connolly**

Introduction

Networked resources, including Internet access, are available to all pupils 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.

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 will only be permitted upon receipt of signed permission. 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 The Leader of Learning Technologies.

Acceptable Use

Users are expected to use 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 The Leader of Learning technologies
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 the Leader of Learning Technologies
10. Staff should use cloud based technologies for storage purposes outside school e.g. dropbox.com, one drive or google drive. USB storage drives should not be used, (Permission must be sought from the Headteacher before use. They must be checked for viruses each time they are used and be password protected / encrypted in line with GDPR compliance expectations.)
11. 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 on the computer. Downloading some material is illegal and the police or other authorities may be called to investigate such use.

12. Files held on the school's network will be regularly checked by the Leader of Learning Technologies or class teachers (in the case of pupils).

13.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 offensive 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.
- 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.

- Unless authorised to do so by the Computer Technician or the Leader of Learning Technologies users must not download software onto the network. Staff have the ability to download software locally onto their staff laptop, however if they need it on the network they must raise a ticket so the installation can be checked for network security. All laptops should be pass word protected to ensire confidentiality and GDPR compliance.

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 the Leader of Learning Technologies immediately if a security problem is identified and 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.

SOCIAL MEDIA

Please refer to the separate social media policy. The school is currently setting up a Facebook this will be administered for information purpose about the school by the Leader of Learning Technologies and the Assistant Head Teacher

Children of primary school age should not have a Facebook account or any other social media account where the age limit is above that of their age.

HOW WE MANAGE THE INTERNET.

There are three main levels of management, each is as important as the other and all work together to provide for our internet safety.

1. Staff observing.
2. Filtering (SWURL).
3. Forensic Software.

1. ***STAFF OBSERVING.***

Observation and supervision by staff is important. During web searches or when linking to new sites/pages unsuitable material may be accessed. It is up to staff to be vigilant and supervise children when the internet is used.

In the initial weeks of the school year before pupils actively use any technology all pupils will be reminded of the school system for reporting anything they read or see online that makes them feel uncomfortable.

- ***Cover the screen*** – Laptop lids closed / iPads turned over (The site is left up so staff can take appropriate action and no other pupil is effected)
- ***Tell an adult*** – They must report this to the teacher straight away.

Further etiquette and internet safety will be built into units of work throughout the school year to teach responsible safe e-citizens.

Staff should note any inappropriate site visited and pass the information to the Leader of Learning Technologies for further action. Year Leaders or Assistant Head Teachers may need to be involved in talking to parents of pupils who have seen anything that is inappropriate.

2. *FILTERING*.

This system filters sites based on a list that is regularly reviewed and updated by our internet service provider. Additional Sites removed from the filter by the Head Teacher, Assistant Head Teacher or Leader of Learning Technologies - once the site has been review and deemed acceptable for use. Any sites added to our filter will be reported to our Internet Provider for them to review for other schools.
This is a 'global' systems that manages many LEA schools and as such denies access to sites that may be deemed OK by some schools but not others.

3. FORENSIC SOFTWARE.

This system works on two levels.
It controls access to sites based on their content (words or pictures) or those on a list.
It also allows the designated staff to review what websites have been visited, when and by whom.

This tracking is manageable by the school and will be reviewed on a regular basis.

INTERNET ACCESS INFRINGEMENT.

Staff Access will be managed by the Head teacher and any access deemed as unsuitable or inappropriate will be dealt with accordingly by him/her in accordance with school staff management procedures.

Pupils Access will be managed by the Leader of Learning Technologies.
Any pupils seen to be accessing or trying to access inappropriate sites should be dealt with in the following manner as soon as possible after the event.

1. Pupil name to be passed to Leader of Learning Technologies for tracking purposes using Forensic software.
2. Sites accessed to be noted by staff member (if possible) and /or the computer used to be noted (for tracking and management purposes).
3. Year Leader or AHT to be informed.
4. Head teacher to be informed and they will decide if further action is required.

Questions to consider:
Was the access accidental? If so how (sites search, link for another site etc).

Was this a deliberate access (Site address brought in from home for example)?
Has this pupil done this before?
What was the content of the site? (To help deem suitability.)

MEDIA PUBLICATIONS

Written permission from parents or carers will be obtained before named photographs of pupils are published.

Publishing includes, but is not limited to:

- the school website and Learning Platform,
- Classroom blogs,
- the Local Authority web site,
- web broadcasting,
- TV presentations,
- Internal School Television system,
- Newspapers.

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

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.