LITTLE HARROWDEN COMMUNITY PRIMARY SCHOOL

POLICY FOR: ICT Acceptable Use

Responsible person: Mrs J Foo

Date adopted: September 2020 **Review by:** September 2021

Introduction

The internet is an essential element in 21st Century life for education and social interaction. The purpose of internet use in school is to promote pupil achievement, to support the professional work of staff and to enhance the school's management, information and business administration system. Benefits include:

· Access to world-wide resources and research materials

· Educational and cultural exchanges between pupils world-wide (Skype for instance)

· Access to experts in many fields

· Staff professional development, such as access to online learning and forums

· Communication with support services, professional associations and colleagues

· Exchange of curricular and administration data (i.e. between colleagues, LA and DfE)

The statutory curriculum requires pupils to learn how to locate, retrieve and exchange information using ICT. Consequently, in delivering the curriculum teachers need to plan to integrate the use of ICT and web based resources including e-mail to enrich learning activities. **Effective internet use is an essential life skill.**

Access to the school's ICT network and use of ICT facilities owned by the school, including access to the Internet, are conditional on observance of the following Acceptable Use Policy. The Aims of this Acceptable Use Policy are to:-

- Allow all users access to school ICT resources and use of the Internet for educational purposes.
- Provide a mechanism by which staff and pupils are protected from Internet sites, information, and individuals that would undermine the principles and aims of the school.
- Provide rules which are consistent, and in agreement with the Data Protection Act 1984, Computer Misuse Act 1990 and other legislation relevant to the use of computers and electronic data in schools.
- Provide rules that are consistent with the acceptable procedures commonly used on the Internet, including those associated with netiquette.
- Provide rules relating to the use of computers and ICT facilities in school, which are consistent with the general policies of the school.

General Internet use and Consent

Pupils who are to have access to the internet must understand the basic conventions and navigation techniques before going online and accessing material.

Pupils must not use the school ICT facilities without the supervision of a member of staff. Although use of the ICT facilities and access to the Internet will be supervised, and all possible measures will be taken (including the use of Exa Internet Service provider, filtering and firewall), Little Harrowden Primary School and Northamptonshire County Council cannot accept liability for the accessing of inappropriate materials or any consequences of internet access.

If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the ICT Subject Leader and Technician immediately who will, in turn, record the address and report on to the Headteacher and Internet Service Provider.

Pupils are aware that they must only access those services they have been given permission to use.

Staff and pupils are made aware that the use of computer systems without permission or for inappropriate purposes is a criminal offence (Computer Misuse Act 1990).

Staff and Governors must agree to and sign the Acceptable Use Agreement (appendix) each year.

Log in and Passwords

Pupils and staff must not disclose any password or login name given to anyone, or allow anyone else to use a personal account.

Staff and pupils must ensure laptops are logged off (or hibernated) when left unattended.

Adult users are expected to be in charge of their own areas on the network. Passwords are therefore set for each user.

Blogs

The school recognises the importance of children having a positive online profile and an understanding of how social media can support them in the future. In order to teach this, the school has a blog space which can be accessed by the public. This gives children the opportunity to develop their skills in a relevant and immediate forum, allowing them access to a large audience. School understands that it acts as a model for how to manage an online profile successfully. The blog is mediated and only suitable content is uploaded. Children can contribute content at home and at school and parents and friends are actively encouraged to give supportive feedback. In order to contribute to blogs at home, children will need an email address. School will provide an email address to each child. These can be changed at home and managed by parents. All contributors will follow online profile rules below:

1. Don't write your surname on any post
2. Only write positive comments, don't be mean or offensive
3. No swearing or using rude words
4. Don't write your address or any other person's address or other identifying information
5. No text talk – please make sure you write in full sentences and check your replies before sending them.
6. Parents – please be careful not to use pupil surnames or make comments which identify pupil surnames

Youtube

The school has a Youtube account and will post videos on school blogs and the website using this account, following Acceptable User protocols, including checking parent permissions. In order to reach wider audiences and demonstrate the power of positive social media, we may share videos via Twitter or Facebook using the school accounts. Surnames and personal information that could identify a specific child will not be used. In this way school will act as a model for keeping safe on-line whilst allowing children the freedom to understand the power of social media.

General Safety and Risk Assessment

The consumption of food or drink is forbidden whilst using a computer. It is hazardous to the equipment and to individuals.

Users must treat with respect equipment and services in school and at other sites accessed through school facilities, and are subject to regulations imposed by the respective service providers. Malicious action will result in immediate suspension from use of the school facilities.

Cyber-Bullying (see Anti-Bullying Policy and E-Safety Policy)

The experience of being cyber-bullied can be very painful for those who are the targets. **Adults need to help children and young people prepare for the hazards of using technology while promoting learning and social opportunities.** Some forms of cyber bullying are different from other forms:

- Through various media children can be cyber-bullied 24 hours a day.
- People who cyber-bully may attempt to remain anonymous.
- Anyone of any age can cyber-bully.
- Some instances of cyber-bullying may be unintentional – such as a text sent as a joke or an email to the wrong recipient.

Prevention

We recognise that the best way to deal with cyber-bullying is to prevent it from happening in the first place. By embedding good, safe ICT practice into all our teaching and learning, incidents can be avoided.

We recognise we have a shared responsibility to prevent incidents of cyber-bullying but the Headteacher has the responsibility for coordinating and monitoring the implementation of anti-cyber- bullying strategies.

Understanding Cyber-bullying

The school community is aware of the definition of cyber-bullying and the impact cyber-bullying has.

Staff receive guidance and review the Anti-Bullying and Acceptable Use Policies regularly. Children are taught how to recognise cyber-bullying and their responsibilities to use ICT safely. ICT safety is integral to teaching and learning practice in the school.

Parents are also taught how to recognise cyber bullying and their responsibilities for supporting safe ICT use and are asked to refer to the Thinkyouknow website yearly at the beginning of the year.

Record Keeping and Monitoring Safe Practice

As with other forms of bullying, the Headteacher keeps records of cyber-bullying. Incidents of cyber-bullying will be followed up using the same procedures as other forms of bullying.

E-Safety

Children and staff are reminded of E-Safety Codes of Conduct at the start of each academic year.

Any work or activity on the Internet must be directly related to schoolwork. Private use of the Internet (including social networking sites) in school is strictly forbidden.

Staff are discouraged from being members of social networking sites. However, if staff are members they are reminded of the necessity to keep their profiles secure and to avoid contact with persons (particularly parents/pupils or ex-pupils) related to the school. Staff are reminded that any action or comment that brings the school or colleagues into disrepute or compromises pupil or staff confidentiality will be classed as a disciplinary matter.

Do not give personal email or postal addresses, telephone / fax numbers to any person.

Under no circumstances give email or postal addresses / telephone numbers / fax numbers of any teachers or pupils at school.

Distribution of computer viruses, electronic chain mail, computer games, use of Internet Relay Chat and similar services are strictly forbidden by pupils and staff as they can result in degradation of service for other users and increase the workload of the IT staff.

Do not download, use or upload any material that is copyright. Always seek permission from the owner before using any material from the Internet. If in doubt, or you cannot obtain permission, do not use the material.

Users should assume that ALL software is subject to copyright restrictions, including shareware. Pupils must not, under any circumstances download or attempt to install any software on the school computers. Staff should seek the advice of the ICT technician or the ICT Subject Leader before attempting to download or upload software.

Under no circumstances should users view, upload or download any material that is likely to be unsuitable for children or schools. This applies to any material of violent, dangerous, racist, or inappropriate sexual content. If users are unsure about this, or any materials, users must ask teachers or ICT co-ordinator. If in doubt, DO NOT USE. The transmission, storage, promotion or display of offensive, defamatory or harassing material is strictly forbidden as they breach the laws of the UK under the Computer Misuse Act. Possession of certain types of unsuitable material can lead to prosecution by the police.

Off-site pupil data and pupil information

Lap tops, staff Ipads and back-ups (USB sticks) may be taken off site. Staff are to ensure that lap tops are used cautiously when viewing pupil data/information and images and that lap tops are logged off when left unattended. Back Ups to hold pupil data or images should be in the form of encrypted USB pens. Images must be transferred to the school network as soon as possible to be removed within the set timescales. Data, images and pupil information from previous years should be removed from back- ups and stored on the school network to avoid unnecessary information being kept on portable devices.

Virus Checks

All computers in school have anti virus software, although very new viruses will not be found. If you suspect a virus please report it to the ICT technician straight away and/or record in the ICT problem book if ICT Technician is not available.

E-Mail Usage

Use of e-mail and communication by e-mail should be treated with the same degree of care you would take if you wrote a letter to the person that you are contacting by email. It cannot be regarded as purely private, only to be seen by the receiver. E-mail can be stored, forwarded and distributed to large numbers of people at the touch of a button. It is easy to forget that it is a permanent form of written communication and that material can be recovered even if seen to be deleted from the computer

When using e-mail, pupils and staff should:

· Not access personal emails in school using school equipment.

· Be aware that e-mail is not a secure form of communication and therefore pupils should not send ANY personal information.

· Should not attach large files

· Must not forward e-mail messages onto others unless the sender's permission is first obtained.

· Must not open e-mail attachments from unknown senders or from computers from which virus protection may not be current or activated

· Not send e-mail messages in the heat of the moment and avoid writing anything that may be construed as defamatory, discriminatory, derogatory, rude or offensive.

· This Guidance will apply to any inter-computer transaction, be it through web services, chat room, bulletin and news group or peer to peer sharing.

<u>Mobile Devices</u>

Pupils are not permitted to bring mobile phones or devices in to school. Should there be a need for a child to bring their device in to school this should be turned off and handed to the School Office to look after during the school day and collected at 3.15pm.

Pupils may not make personal calls from a mobile phone during the school day.

Mobile phones may not be used to take pictures of pupils and staff (use class Ipads /cameras provided by the school)

Pupils should not send or receive email or text messages to/from their mobile device during the school day.

Any inappropriate use of mobile devices such as cyber-bullying must be reported to the Headteacher (see anti-bullying policy).

Staff should only use their mobile phones at appropriate times of the day only e.g. break times. During the school day their mobiles should be turned off or set to silent. Staff must not use personal mobile devices or cameras to take images of pupils or staff.

<u>Legal Requirements</u>

Users must agree to comply with all software license agreements. Do not attempt to copy any software from, or by using school computers. If you have any requirements for using additional software for any reason, please contact the ICT technician to discuss the situation. Solutions are possible! Remember also that shareware is not freeware and must be licensed for continued use.

Computer facilities shall not be used to hold or process personal data except in accordance with the provisions of the Data Protection Act 1984. Any person wishing to use the facilities for such a purpose is required to inform the Headteacher in advance and comply with any restrictions that the school or the UK Data Protection Registrar may impose concerning the manner in which data may be held or processed.

Copyright Designs & Patents Act - Copyright is infringed if a person acquires an unauthorised copy of a computer program. Mere acquisition, without regard to the actual or intended use, constitutes an infringement of the author's copyright. "Acquisition" includes loading a copy of a programme into the random access memory, or other temporary storage device, of a computer, or onto any form of permanent data storage medium.

The high cost of commercially marketed software and the ease with which it can be copied make it tempting to copy software illegally. Agents for software developers are aggressively seeking to protect their rights under the law. Schools can be audited at anytime. Anyone found to have unauthorised copies of software will immediately be suspended from using the IT facilities. The matter will be investigated and the necessary action taken, the school will not accept any liability whatsoever.

"Hacking" is illegal under the Computer Misuse Act 1990. Regulations regarding unauthorised access or misuse of computing facilities are enforceable under the law, any person found attempting to or hacking the school network will be prosecuted.

Regulations regarding the transmission, storage or display of obscene material are enforceable by law under the Criminal Justice and Public Order Act 1984 which amends the Obscene Publications Act 1956, the Protection of Children Act 1978 and the Telecommunications Act 1984 to extend their provisions to transmission over a data communications network.

Sanctions

If pupils break the rules as laid down by this policy they will lose temporary or permanent use of the school systems. Parents will be informed and if the law has been broken the police will be informed and the school will assist the police with any prosecution.

If staff break the rules as laid down by this policy they will lose temporary or permanent use of the school systems and will be subject to disciplinary proceedings. If the law has been broken the police will be informed and the school will assist the police with any prosecution.

Pupils with Additional Learning Needs

The school strives to provide access to a broad and balanced curriculum for all learners and recognises the importance of tailoring activities to suit the educational needs of each pupil. Where a pupil has specific learning requirements, or poor social understanding, careful consideration is given to the planning and delivery of e-safety awareness sessions and internet access.

Named Personnel

Our Named Governor for ICT Acceptable Use is _____

The Person Responsible for E-Safety and Acceptable ICT Use is the Headteacher

Review – December 2015

Approved by_____(Chair of Governors) Date _____

Acceptable Use Agreement for Staff and Governors

This agreement applies to all online use and to anything that may be downloaded or printed.

All adults within the school must be aware of their safeguarding responsibilities when using any online technologies, such as the internet, E-mail or social networking sites. They are asked to sign this Acceptable Use Agreement so that they provide an example to children and young people for the safe and responsible use of online technologies. This will educate, inform and protect adults so that they feel safeguarded from any potential allegations or inadvertent misuse themselves.

- I know that I must only use the school equipment in an appropriate manner and for professional uses.
- I understand that I need to obtain permission for children and young people before they can upload images (video or photographs) to the internet or send them via E-mail.
- I know that images should not be inappropriate or reveal any personal information of children and young people.
- I have read the procedures for incidents of misuse in the ICT Acceptable Use Policy so that I can deal with any problems that may arise, effectively.
- I will report accidental misuse.
- I will report any incidents of concern for a child or young person's safety to the Senior Designated Person in accordance with procedures listed in the Acceptable Use Policy.
- I know who my Senior Designated Person is.
- I know that I am putting myself at risk of misinterpretation and allegation should I contact children and young people via personal technologies, including my personal e-mail. I know I should use the school e- mail address and phones to contact parents and school equipment only when taking photos ofchildren.
- I know that I must not use the school system for personal use unless this has been agreed by the Headteacher.
- I know that I should complete virus checks on my laptop and memory stick or other devices so that I do not inadvertently transfer viruses, especially where I have downloaded resources.
- I will ensure that I follow the Data Protection Act 1998 and have checked I know what this involves, including password protecting memory sticks.
- I will ensure that I keep my password secure and not disclose any security information unless to appropriate personnel. If I feel someone inappropriate requests my password I will check with the Headteacher prior to sharing this information.
- I will adhere to copyright and intellectual property rights.
- I will only install hardware and software, including Apps, I have been given permission for by the Headteacher.
- I accept that the use of any technology designed to avoid or bypass the school filtering system is forbidden. I understand that intentional violation of this rule may result in disciplinary procedures being initiated.
- I have been shown a copy of the Acceptable Use Policy to refer to about all e-safety issues and procedures that I should follow. A copy can be found on the school website.

I have read, understood and agree with these Agreement as I know that by following them I have a better understanding of e-Safety and my responsibilities to safeguard children and young people when using online technologies.

Name:_____

Sign:_____

Date:_____