At Lobley Hill Primary School we aim to 'Be the Best We Can Be' through being curious, adventurous and respectful in order to achieve personal excellence.

Lobley Hill Primary School (incorporating Gateshead Primary SCITT)

Computing Acceptable Use and Data Protection Policy

Approved by:	Governing Body	Date: September 2021
Last reviewed on:	July 2021	
Next review due by:	July 2022	

Mission Statement

At Lobley Hill Primary we aim to 'Be the Best We Can Be' through being curious, adventurous and respectful in order to achieve personal excellence.

School vision

We want to provide an inspirational and welcoming environment where all children are respected, feel happy, safe and secure in their learning. We promote an inclusive and effective learning community where we celebrate diversity and have high expectation for all.

We want to enhance children's life chances through a stimulating supportive partnership with parents and carers that nurture each child to achieve his/her full potential and we achieve this through a creative holistic approach in all that we do.

We want our children to become responsible, confident members of a global society who can apply their experiences gained at Lobley Hill Primary School to all future learning.

Contents

Computing Acceptable Use Policy

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 trainees and to enhance the school's management, information and business administration system. Benefits include:

· Access to worldwide resources and research materials

· Educational and cultural exchanges between pupils worldwide

· Access to experts in many fields

· Staff and trainees 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)

Internet use and access in Lobley Hill Primary School is considered a privilege. Therefore, if the school AUP is not adhered to this privilege will be withdrawn and appropriate sanctions, as outlined below, will be imposed.

It is envisaged that staff and a governor will revise the AUP annually. Before signing, the AUP should be read carefully to ensure that the conditions of use are accepted and understood. This policy has been revised in line with new General Data Protection Regulations (GDPR) to ensure all staff, trainees and Governors are aware of its principles, mandatory requirements and implications.

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.

Parents wishing their children's photos to be excluded from use in booklets, advertising and on the website will be required to provide a formal, written statement of omission. If a picture is placed on the website the child's full name will not be displayed.

Pupils must not use the school computing facilities without the supervision of a member of staff. Although use of the computing facilities and access to the Internet will be supervised, and all possible measures will be taken Lobley Hill Primary School cannot accept liability for the accessing of inappropriate materials or any consequences of internet access.

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

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

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

Log in and Passwords

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

Staff, trainees and pupils must not attempt to gain access to the school network or any Internet resource by using someone else's account name or password.

Staff, trainees and pupils must ensure desktops or laptops are logged off (or locked) 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. We recommend that passwords are changed frequently. Passwords should be over 4 characters and should contain letters, numbers and symbols. They should not contain spaces.

To protect your work area do not tell anyone your password. The password is displayed on screen as a line of ******, however people watch fingers and it is quite easy over a period of time to work out what the password is, so be careful. Anyone who needs assistance in changing their password should contact the ICT technician (Omnicom).

General Safety and Risk Assessment

The consumption of food or drink is forbidden whilst using a computer. It is potentially hazardous to both 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.

Risk assessments are completed for use of iPads, iPad trolleys, laptops and laptop trolleys and are kept in the secure suite. Staff and trainees are responsible for sharing the safety issues with their pupils.

Clear Desk Policy

It is the responsibility of all employees to ensure no data information is left on their desk at the end of the school day. All information must be placed in a secure location or filed correctly to prevent any GDPR incidents.

Cyber Bullying (see Anti-Bullying 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 computing 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 internet safety officer together with the Headteacher has the responsibility for co-ordinating 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 and trainees receive guidance and school staff review the Anti-Bullying and Acceptable Use Policies regularly. Children are taught how to recognise cyber bullying and their responsibilities to use computers safely. Computer 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 computing during annual internet safety meetings and information leaflets throughout the year.

The school runs a regular termly assembly focusing on cyber bulling and internet safety.

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. However, we recognise to monitor internet use on a regular basis as a disincentive for bullies misusing school equipment and systems. The ICT technician (Omnicom) will conduct regular use checks, log any concerns and inform the Headteacher.

Internet Safety

Staff, trainees and pupils are reminded of the Acceptable Use Policy at the start of each term. The first computing session of each half-term should be based on internet safety. Every year, parent/child internet safety sessions will be led in school. Internet safety guidance will also be handed out throughout the year to ensure parents are aware of the importance.

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 on the school network.

Under no circumstances do Staff, trainees and pupils give email or postal addresses/telephone numbers of any teachers, trainees or pupils at school to members of the general public.

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 ICT 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. Staff, trainees and pupils must not, under any circumstances download or attempt to install any software on the school computers. Staff and trainees should seek the advice of the ICT technician (Omnicom) or the ICT Co-ordinator 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, homophobic 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.

Social Networking

Staff and trainees need to be aware of the risks involved with social media and social networking sites. If staff and trainees are members of any social networking site, they are reminded of the necessity to keep their profiles secure and to avoid unnecessary contact with persons (particularly parents/pupils or ex-pupils) related to the school. Staff and trainees are reminded that any action or comment that brings the school or colleagues into disrepute or compromises pupil, staff or trainee confidentiality will be classed as a disciplinary matter.

The school Facebook site is used as a form of communication for parents and is run by Johanna James (Headteacher). All parents are given the opportunity to state whether they would like their child's photograph to go onto social media sites. Johanna James is to check everything that is posted on Facebook against the list of children's names for permission to be allowed on social media. Johanna James must accept every 'post' before

it is entered onto the Facebook 'timeline' to ensure it is suitable to be viewed by members of the public. Staff and trainees are able to be part of the Facebook site, however they must ensure that their profile is private and any comments that are made are appropriate. The school has their own Twitter account. Any action on the social media account will monitored closely. (Refer to Social Media Policy)

It is unacceptable for pupils attending Lobley Hill Primary School to be members of Social Networking sites. The majority of Social Networking Sites have a minimum age limit of 13. The children of Lobley Hill Primary School do not meet this minimum requirement. We look to parents and carers to support the school with this ethos.

Gaming

Children accessing online games in school will only do so with the direct support and supervision of a member of staff. Such gaming activity will be relevant, planned for and provide progression in learning. Children accessing online games at home are at risk due to other gamers misrepresenting themselves and gaining information about the child. Parents and carers experiencing difficulties at home will be supported by the internet safety Officer and referred to http://www.thinkuknow.co.uk/parents/

School Network and Pupil Files

Always respect the privacy of files of other users. Do not enter the file areas of other users without obtaining their permission first (unless there is reasonable question over the content of the files). Files to be shared should be saved to the Staff Shared Area (Q:). Pupils can access and save work to their own log-on through the server; this can only be accessed by that child and the ICT technician (Omnicom).

Do not modify or delete the files of other users on the shared areas without obtaining permission from them first.

The ICT technician (Omnicom) will view any material pupils store on the school's computers, or on memory sticks/disks pupils use on the school's computers.

Storage space on the network is limited. All users are requested to ensure that old unused files are removed from their area at the end of each academic year. In line with GDPR legislation anything that is not required to be retained should be removed. Hard drives are provided for each Key Stage to store any important documents from previous years. Users unsure of what can be safely deleted should seek advice from the ICT leader or ICT

technician (Omnicom). In exceptional circumstances, increased storage space may be allowed by agreement with the ICT technician (Omnicom).

Users accessing software or any services available through school facilities must comply with licence agreements or contracts relating to their use and must not alter or remove copyright statements. Some items are licensed for educational or restricted use only.

Be polite and appreciate that other users are entitled to differing viewpoints. The use of strong language, swearing or aggressive behaviour is forbidden. Do not state anything that could be interpreted as libel.

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 internet safety awareness sessions and internet access.

Security Guidelines

Backups

Files stored on the network are backed up regularly by Omnicom. This means files can be restored if deleted or lost in error. However, if you create and delete files on the same day then a backup will not be available to restore. Backups are kept securely by Omnicom at a data centre.

Save Regularly

It is very important to save work regularly (approx. every 10 minutes). The network is very reliable but problems do occur i.e. programs crash, power failures. If work is saved regularly and a PC or the network does fail for any reason, only the work done since the last save will be lost. (See above)

Offsite pupil data and pupil information

Staff should sign an agreement and this AUP at the beginning of the academic year which will allow them to take their staff iPad offsite, these iPads will be password protected but staff are responsible for ensuring that they are used cautiously and stored in a safe place whilst offsite. Backups (Encrypted USB sticks only) may be taken off site. Backups to hold pupil data or images should be in the form of encrypted USB pens, if any member of staff

is unsure of how to do this, they should seek support from the ICT technician (Omnicom) or the Computing co-ordinator. If laptops need to be taken offsite, permission needs to be given from the SBM, hardware should be signed out if it is taken offsite. Staff are to ensure that laptops are used cautiously when viewing pupil data/information and images and that laptops are logged off when left unattended. Images must be transferred to the school network as soon as possible to be removed within the set timescales. Data, images and pupil information must be removed from backups and laptops when pupils transfer to another class to avoid records being kept of pupils that are not taught by their former teacher.

Virus Checks

All computers in school have antivirus software, although very new viruses will not be found. If you suspect a virus please report it to the ICT technician (Omnicom) straight away in the ICT problem book.

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:

- Be aware that e-mail is not a secure form of communication and therefore pupils should not send ANY personal information.
- Not use personal e-mail addresses, unless security protected
- 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
- Must 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 rooms, bulletins or texting.

Mobile Devices

Pupils are not permitted to bring mobile phones or devices into school. Should there be extenuating circumstances, which mean there is a need for a child to bring their device in to school, school need to be informed by the parent/carer and the mobile should be turned off and handed to the School Office to look after during the school day and collected at the end of the school day.

Pupils may not make personal calls from a mobile phone during the school day. Pupils should not send or receive email or text messages to/from their mobile device during the school day.

Mobile phones may not be used to take pictures of pupils and staff (use iPads provided by the school).

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

Any pupil who is seen with a mobile device during the school day will have it removed from them to be collected at the end of the school day (in accordance with the school's Behaviour Policy). The device will be secured in a safe location.

Smart Watches

Staff are permitted to wear Smart Watches during the school day, however they must be disconnected to mobile phones or set to airplane mode.

Staff should only use their own 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. The Headteacher reserves the right to request to view any photographs stored on mobile devices brought into school.

Video-Conferencing and Webcams

Taking images via a webcam should follow the same procedures as taking images with a digital or video camera.

Permission should be sought from parents and carers if their child is engaged in video conferencing with individuals or groups outside of the school. This process should always be supervised by a member of staff and a record of dates, times and participants held by the school.

Children need to tell an adult immediately of any inappropriate use by another child or adult. (This is part of the Acceptable Use Agreement).

Where children, young people (or adults) may be using a webcam in a family area at home, they should have open communications with parents/carers about their use and adhere to the Acceptable Use Agreement.

Legal Requirements

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 (Omnicom) 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 Head Teacher 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 ICT 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.

Further Support & Guidance

Websites linking to e-safety and Acceptable Use:

http://www.thinkuknow.co.uk/

http://www.ceop.police.uk/

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.

Managing Allegations against Adults Who Work With Children and Young People

In order to deal with any incidents that occur as a result of using personal mobile or e-mail technologies we will be referred to Gateshead LA. The procedures detail how to deal with allegation of misuse or misconduct being made by any member of staff or child about a member of staff.

Allegations made against a member of staff should be reported to the e-safety officer and Head Teacher within the school immediately. In the event of an allegation being made against the Head teacher, the Chair of Governors should be notified immediately.

Disciplinary Procedure for All School Based Staff

In the event that a member of staff may be seen to be in breach of behaviour and good conduct through misuse of online technologies, this policy outlines the correct procedures for ensuring staff achieve satisfactory standards of behaviour and comply with the rules of the Governing Body.

Data Breach

In the event that any breach occurs resulting in high risk to the rights and freedom of individuals (this may include: unauthorised access to or alteration to data, loss or unlawful destruction, unauthorised disclosure or access to personal data) it must be reported within 72 hours to the Information Commissioner's Office (ICO) and Data Protection Officer (DPO).

Named Personnel

Our Named Governor for ICT Acceptable Use and Data Protection is Ray Shirley

The Persons Responsible for Internet Safety and Acceptable Use are Johanna James (Headteacher) and Karen Turland (Internet safety officer)

Information Commissioner www.ico.org.uk

Data Protection Officers: DPO@Gateshead.gov.uk

Acceptable Use Agreement for Parents, Staff, Trainees and Governors 2021

This agreement applies to:

- All online use
- All data, information, photographs, documentation related to Lobley Hill Primary School and Gateshead Primary SCITT
- Any documentation, information that can be accessed in relation to Lobley Hill Primary School and Gateshead Primary SCITT
- Any documentation that can be downloaded or printed
- Use of any mobile, personal or work-related technology

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 and data. This will educate, inform and protect adults so that they feel safeguarded from any potential allegations or inadvertent misuse themselves.

All adults within school must be aware of their responsibility when accessing data, documentation and sensitive information in ensuring this is used only for its intended professional purposes.

- 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 email.
- 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 Lobley Hill Primary School Computing Acceptable Use Policy so that I can deal with any problems that may arise, effectively.
- I will report accidental misuse immediately to Johanna James (Headteacher)
- I will report any incidents of concern for a child or young person's safety to the e-safety officer in accordance with procedures listed in the Acceptable Use Policy.
- I know who my Internet safety officer 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.
- 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 GDPR 2018 and have checked I know what this involves.
- 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 I have been given permission for.

- 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 agree to delete any records, photographs, data or information relating to school from my personal PC, laptop, phone, Ipad, hard drive or non-encrypted memory devices.
- I agree to use only encrypted memory pens to hold information in relation to school and only to store information that is absolutely necessary – all other information and data will be transferred to the school server
- I agree not to download information from sites such as Behaviour Watch to any of my personal devices
- I agree not to share records, photographs data or information relating to school via personal email, social media, drop box or any other sharing medium.
- I agree to only send information in relation to school via secure email.
- I agree to only remove from school books, data and information that is absolutely necessary to my role and to ensure it is transported securely, stored safely and returned when no longer in use.
- I agree to ensure any records, data and information are destroyed in the appropriate manner when no longer in use.
- I have completed GDPR training and understand my responsibility in ensuring data is protected and used only for its intended purposes.
- I have a better understanding of Internet Safety, Data Protection and my responsibilities to safeguard children and young people when using online technologies.
- I agree to return my fob and encrypted memory stick at the end of my contract.
- I agree to return any data which has been collected or collated for the purposes of training or placement, to SCITT at the end of each placement.
- I agree not to allow any pupil to have access to my fob on or off site.
- I agree to collect all documents and data from the photocopier when sent through to print.
- I agree to lock my computer when I am away from my workstation for any length of time.
- I have read, understood and agree with this document.

Signed……. Date…….

Name (printed)…….