Lakeside School

ICT Acceptable Use Policy

Contents

Appendix

ICT Acceptable Use Policy

1 Introduction

This policy sets out the acceptable use of Information and Communication Technologies within Lakeside School.
Copies of this document are available in the school office or on the website.

2 Definition of Terms

The following terms are used in this document and relate to the following:
Network User – any person that uses the schools network infrastructure.
Staff – any employee of the school or visiting consultant, adviser or other visitor to the school.
Student – any person who attends the school for education purposes
Hacking – any attempt to bypass any of the school network's security features
The School – Lakeside School
AUP – Acceptable Use Policy

3 School-wide policies and procedures

The Schools' AUP is part of a suite of documentation which covers the safe and legal use of ICT within the school. These include child safety, anti-bullying, health and safety, data protection act, fair processing and copyright.

Use of ICT is monitored within the school, and cases of misuse by staff and students will be reported to the Head Teacher. A log of incidents is maintained by the ICT Co-ordinator. The AUP will be reviewed at least every 4 years, and more frequently if a need for change is identified.

The SLT and ICT Co-ordinator will oversee the development and implementation of Internet safety policies at Lakeside School.

4 Communication with parents and carers

Parents are contacted directly where concerns exist regarding improper use of the Internet or schools' ICT equipment. Improper use may result in students being banned from using the system and other disciplinary measures may be taken depending upon the nature of the abuse (e.g. Detention or Exclusion from school)

5 Acceptable use guidelines for staff

Any school computer equipment or service utilised by a member of staff is provided for the primary purpose as a work tool, for work related duties only. It must not be used to conduct a personal business/enterprise for personal gain.

Staff must keep their passwords secure and make sure their passwords are of significant strength. They should include a mixture of upper case, lower case and numbers to make it difficult for anyone to guess. Passwords must not be given to any other members of staff or students.

Staff are responsible for the security and acceptable use of their laptop/network account. Staff must ensure that their laptop and other computer equipment is stored securely when not in use. Staff must not keep passwords with their laptop. If a laptop is lost or stolen, the Head teacher and ICT Co-ordinator should be informed immediately so that appropriate action can be taken.

Laptops connected to the school network allow staff to access their network area. Any work stored in the network area is backed up automatically. If the laptop is used when not connected to the network, any work created is saved onto the laptops hard drive and is not backed up by the school system. Staff should take care to ensure this work is transferred to their network area the next time they connect to the school network to prevent data loss.

Staff must not keep ‘personal information’ about students on their laptops in case of theft – data such as contact details etc should not be stored on laptops.

All software must be installed by the ICT Co-ordinator and must have the relevant license made available to them before installation. Software without the correct license must not be installed and staff who attempt to install software themselves will be responsible.

The ICT Co-ordinator maintains a software audit, containing a list of the software installed on each computer or laptop.

This audit will be made available to any official body who require it for the purposes of copyright enforcement. The use or copying of software without the licensor's permission is illegal and equally the terms and conditions of software licenses must always be adhered to.

The copying of music files, video and other copyright material if not legally purchased by the member of staff onto school computers may be illegal and removed if discovered. DVD’s may only be played to an audience if it is within the terms of their license agreement.

Whilst it is the user’s responsibility to take reasonable care over the configuration of their computer hardware, it is possible for software to be installed on a machine without the full comprehension of the user. Users discovering software that has been installed in an unsolicited manner and which contravenes the licensing regulations above must contact the ICT Co-ordinator who will assist in resolving any issues.

The school has the right to request access to or reclaim any laptop or computer without explanation. The Headteacher and ICT Co-ordinator have the ability to view all files on the network.

Staff are responsible for backing up data when they end their employment with the school. Staff must be aware of the Data Protection Act and are prohibited from taking copies of any personal data about students or other members of staff.

Contact with Parents/Guardians should not be made via email and instead should be carried out via phone calls or a formal letter/meeting. Any contact with students via electronic means must be for teaching and learning and must only be carried out via the schools own systems (e.g. School email or VLE system) – this includes not sending emails to student personal accounts and only sending mails to their school email addresses.

No use of personal email/social networking systems etc should ever be used to communicate with students of the schools for child protection and staff protection (e.g. allegations against a member of staff etc).

6 Acceptable use guidelines for students

Students:

- Must only use the own user area and not attempt to access other user's files.
- Must keep their passwords secure and make sure no one else knows it. Passwords should not be easy to guess.
- May only use the computers for school work or home study.
- Must only send e-mails to people known to themselves or with the permission of a member of staff.
- Must only send e-mails that are polite and responsible and must not contain any personal information about themselves.
- Must only use the school email system for school related messages.
- Must report to a member of staff any inappropriate messages they have received. All information will be treated in the strictest confidence.
- Must report any damage to a member of staff immediately
- Must report to a member of staff any inappropriate website, image or video clip if they discover one is accessible from the schools computers.
- Must not attempt to circumvent the Schools proxy server to access websites blocked by the school or LA (For example, using proxy bypass websites to access Facebook, You Tube and other social networks)
- Are subject to checks of their computer and Internet usage. E-mails may also be monitored.
- If students fail to abide by the above conditions, their Internet access will be blocked at the discretion of a senior member of staff. In severe cases network access may be removed.
- Must not attempt to breach the schools network security, intrude into other peoples 'e-space' or attempt to take the identity of another user (e.g. use another students username)

7 Data Protection Act

Data is stored in accordance with the regulations laid out by the Data Protection Act and the Data Protection Policy. We will take every reasonable precaution to protect information. Appropriate physical, electronic and procedural safeguards are in place to ensure the security, integrity and privacy of all information kept in our management information system (MIS). The need for confidentiality will be respected, and sharing of data will only occur with the express permission of parents/carers in line with our fair processing notification. All 'personal data' will only be allowed out of the school with the knowledge of the Headteacher and the ICT Co-ordinator/SLT.

8 Internet safety skills development for students

Internet safety skills are introduced to all students in Year 7 through a teaching unit designed for this purpose. Students receive follow up lessons in Years 8, 9, 10 and 11. Students are made aware through ICT and citizenship of their rights and responsibilities with regard to their use of ICT based technology. This includes issues such as cyber bullying and personal safety.

9 Personally Owned Equipment

Students should not bring personal ICT equipment into school due to the risk of damage or theft. The school cannot be responsible for ensuring the safety of any equipment students do bring with them. Staff wishing to use personal ICT equipment must see the school Caretaker to ensure it is PAT tested before use.

10 Using the technologies safely

10.1 Internet

All Network Users must use their own network account to logon to the network. The School's auditing software automatically records the address of all websites accessed and this information can be retrieved by the ICT Co-ordinator. All Internet access is filtered by Hampshire LA.   Despite all reasonable steps being taken it is possible that unsuitable content could be discovered. In this instance the content should be reported immediately to a member of staff or the ICT Co-ordinator/SLT. Attempts to bypass the filtering system are strictly prohibited and may result in a user's Internet access being removed.

When website issues arise from the school they will be checked against the Internet Watch Foundations banned/illegal website. If deemed necessary the website will be reported to the Internet Watch Foundation and banned through Hampshire Web Filtering.

Responsibilities

The I.C.T Co-Ordinator will hold the responsibility for the management of the school's filtering policy who may delegate this task to a suitable and capable member of the team. They will manage the school filtering, in line with this policy and will keep records / logs of changes and of breaches of the filtering systems.

To ensure that there is a system of checks and balances and to protect those responsible, changes to the HSPN2 / school filtering service must be reported to and authorised by a second responsible person prior to changes being made.

All users have a responsibility to report immediately to the I.C.T Co-Ordinator, the Headteacher or SMT if any infringements of the school's filtering policy of which they become aware or any sites that are accessed, which they believe should have been filtered.

Users must not attempt to use any programmes or software that might allow them to bypass the filtering / security systems in place to prevent access to such materials.

Education / Training / Awareness

Pupils, Staff and Parents will be made aware of the importance of filtering systems through a e-safety education programme, such as the Internet Safety Week that takes place annually through ICT lessons. They will also be warned of the consequences of attempting to subvert the filtering system.

Staff users will be made aware of the filtering systems through:

- Induction training
- Staff meetings, briefings, Inset.

Changes to the Filtering System

If you would like a site unblocked or blocked, you will need to inform the I.C.T Co-Ordinator who will carry out a check on the website to make sure it is safe. If the site is found to be unsafe, it will remain blocked. If you wish to argue the case, this will need to be taken up with the I.C.T Coordinator and the Headteacher.

Users who gain access to, or have knowledge of others being able to access, sites which they feel should be filtered (or unfiltered) should report this in the first instance to the I.C.T Co-Ordinator who will decide whether to make school level changes (as above). If it is felt that the site should be filtered (or unfiltered) at Hampshire County Council (HCC) level, the responsible person should email hantsit@hants.gov.uk with the URL.

10.2 Email

Email Benefits

An email account allows staff to facilitate communications with the LA advisory staff and support services, professional associations and colleagues.

Appropriate Use

Staff need to be aware that emails are easily forwarded so be professional and careful about what you write. All emails should be regarded in the same way as messages on school headed notepaper.

The downloading and sending of copyright material is prohibited.

None of the following should be deliberately sent:

[i] Pornographic language.
[ii] Pornographic pictures.
[iii] Information which may be considered offensive or threatening to others.
[iv] Defamatory or illegal information.

Security

Staff should keep their password confidential and it should not be disclosed under any circumstances.

Staff should change their password occasionally.

Staff may only use their own password-protected accounts to send and check email.

Sensitive information should be sent by post or via a secure transfer system such as LA system (Office 365). Pupil names, details and documents should not be sent via the staff google email accounts or to our link health professionals, when pupil initials are the most that should be used.

Important emails need to be saved securely using a hierarchical file structure; if you need help with this the ICT Coordinator can support you.

Certain emails may need to be printed and saved in pupil files.

Staff must not leave their mailbox open and unattended.

Safety

Only register your email address with reputable organisations.

Never give personal details out over the Internet unless you have initiated the transaction and you are confident of the identity of the receiving party.

Never open, reply or forward spam (junk mail) this includes circular jokes. Inform the school Administrator if you regularly receive junk mail into your account.

Staff who receive inappropriate email need to inform the schools Email Co-Ordinator or HantsIT; the email must not be replied to.

Follow the school guidelines to ensure that the anti-virus on your PC is kept up-to-date.

Be cautious when opening attachments; save any attachments to the computer's hard drive to ensure they are scanned before opening.

Report any problems with your email account to the ICT Department for resolution

Monitoring

The purpose for which monitoring is conducted will be explained fully:

- Your account may be checked for inbox size and/or to check the email system is functioning correctly.
- The content of emails will only be monitored if there is clear evidence that serious misuse has occurred.
- If banned words are sent an automated email will be sent to you and the school administrator to report that this has happened.
- If an email address is sent to a non-existent address (this may occur by typing the email address incorrectly), this will result in a failure message and the contents of your email being returned to the sender; a copy may be sent to the administrator.
- If your email contains a virus, your email is not sent and you and the administrator will receive a copy of the undeliverable email and attachment.

Sanctions

The Headteacher and ICT Co-ordinator will be responsible for ensuring that this policy is implemented effectively. Deliberate misuse of email may after investigation result in disciplinary action being taken against you.

Private Email Use

You are allowed to access personal email accounts, i.e. Hotmail. AOL, Yahoo but only during your time, i.e. your lunch time and not the schools' time.

10.3 Spam and Spoofing

The schools use the Hampshire LA mail filtering service. This service reduces the amount of spam and spoofing emails but users should still be aware of how to recognise spam and spoofing emails and delete them immediately without opening them.

Spam refers to unsolicited email – email that is sent without your permission, usually offering medication or other products such as computer software at lower prices. The subject of a spam message is usually designed to attract people to reading it and therefore you may see subjects such as 'Hot Stock Notice' or 'OEM Software'.

Spoofing refers to an email which claims to be from a bona fide company, such as a bank, requesting that you visit ‘their’ website and confirm your details. Email subjects will often be similar to ‘Regarding Your Online Account’ or ‘Confirm Your Internet Banking Records’. These sites do not belong to the company they claim to be from and subsequently use your details to access your bank account. A genuine organisation would never ask you to confirm details in such a manner.

10.4 Social Networking Sites and Chat Rooms

Staff and Students should not access social networking sites or chat rooms on the school network unless these systems are owned and or managed by the school (e.g. The schools VLE system).

Should Staff or Students wish to set up a social networking site or visit a chat room (or similar) in their own time outside of the schools IT system, they must ensure they do not give away any personal information, such as addresses. For their own protection, the school would like to remind all students to never upload a photo along with their full name or any personal details such as which school they attend.

The School regularly monitors websites to discover any inappropriate material about the School, Staff or other Students and will take appropriate action where necessary.

10.5 Instant Messaging

Student users are unable to install such software and the use of websites offering an alternative are not to be accessed.

10.6 Webcams

Where video conferencing/webcams are used within school, it must be with an authorised third party and overseen by a member of staff. If webcams are used within school it should be with permission of the member of staff in charge and should never be used to record people if they are unaware of the recording. Staff and Students should be aware that certain viruses and Trojans do exist which can activate a webcam without the owners permission.

10.7 Peer-to-Peer (P2P) Networks

Staff and Students are forbidden from connecting to and/or downloading data from peer-to-peer networks.
Peer-to-Peer networks (such as LimeWire, BearShare or Morpheus) often contain copyrighted content, viruses, spyware or other inappropriate materials and users should be aware that downloading files from a Peer-to-Peer network may be illegal or compromise their computer.

11 School websites

The school has its own website. It is the responsibility of the ICT Co-ordinator to ensure that all materials on the school website do not infringe the intellectual property rights of others. The ICT Co-ordinator will take all reasonable steps to ensure that material created by the school is protected under copyright.

The ICT Co-ordinator will ensure that the website is regularly checked for inappropriate content or material and that access to the website server is secured by a strong password to prevent unauthorised access.

The school cannot be held responsible for the content of external sites, even if they are linked to from the school website.

Appendix i

ICT Use Frequently Asked Questions
Introduction

The purpose of this frequently asked question sheet is to give generic examples of acceptable and safe use of the schools ICT systems in accordance with the schools ICT policy. If at any point you are unsure as to what is acceptable or safe then please contact the school's ICT Co-ordinator who can advise.

Q: A student has emailed me from their own personal email address (eg. Hotmail, Googlemail). Can I respond to that email address?
A: You should reply to that student's relevant school email account (ending in for example @Lakeside.hants.sch.uk) and not enter into communication using the external system.

Q: A student has asked me to be their 'friend' on Facebook (or other social networking site/online gaming system – Xbox etc). Can I accept them?
A: No – you should not make or have contact with students via any social networking site or messaging system (such as MSN messenger, Windows Live Messenger, etc)

Q: Students are doing a presentation from my laptop and need my password to logon/remove screensaver. Can I give it too them?
A: No – your password has access to highly sensitive information and must be kept secure. Passwords should include a mix of uppercase letters, lowercase letters and at least one number to make sure they are secure.

Q: I have been asked by an external contact/agency to provide them with a list of students in a year group. Can I send them this information?
A: No – any personal information going to external parties must be agreed by the head teacher or the ICT Co-ordinator. Information is protected under the data protection act and our fair processing notice (on school website). The school must have regards to this before transferring information to any external party.

Q: A parent has emailed me and I need to respond. Can I email them back?
A: No – the response to the email should be made by phone or formal letter (letters must go via the school admin support before going home) and should be discussed with your line manager. Email is not acceptable as a response method.

Q: Can I take my laptop home?
A: Yes – you can take it home and join it to your own internet connection if desired. However, the laptop is for school use and must not be used to conduct a personal business/enterprise for personal gain (tax implications may exist). The laptop must be transported securely and safely. Insurance will only cover the laptop if it is locked away out of sight when transported.

Q: Who is responsible for backing up my laptop?

A: You – to do this go into Lakeside Shortcuts on your desktop and find the link to Backup Laptop. This will store the files on a school server. Laptop drives do go wrong and the ICT Co-ordinator can only get back what exists on your last backup. Staff must ensure that they do this regularly.

Q: Can I install my own software (personally owned or purchased) on to my laptop?

A: You must seek permission from the ICT Co-ordinator – if you wish to have software installed that the school owns then please visit the ICT Co-ordinator.

Appendix ii

Laptop Loan Agreement

Lakeside School Staff: Laptop Loan agreement.

Laptop Make:	<make>
Model :	<model>
Serial Number :	<serial>
Radio Lan Card MAC Address:	<mac address>
Date:	<date>

The laptop detailed above is loaned to ________________ for the duration of their employment at Lakeside School subject to the following terms and the schools' ICT policy. The laptop must be returned to the school on ceasing to be employed at the school.

1. The laptop is for the work related use of the named member of staff to which it is issued.

2. Only software installed at the time of issue or software purchased by and licensed to the relevant school may be installed on the machine.

3. The laptop remains the property of Lakeside School throughout the loan period. However the member of staff to whom it is issued, will be required to take responsibility for its care and safe-keeping.

4. The laptop is covered by the relevant school's Insurance whilst at school. If teaching staff wish to take their laptop home they have to assume full responsibility for it repair or replacement in the event of damage or loss.

5. If left unattended the laptop should be in a locked room or secure area.

6. In order to ensure the schools compliance with the Data Protection Act and to avoid breaches of confidentiality: under no circumstances should students be allowed to use staff laptops. Staff should also be cautious when using the computer away from school particularly with files that may contain personal student data.

7. The laptop will be recalled from time to time for maintenance / upgrade and monitoring.

I have read and agree to the terms and conditions in this agreement.
I undertake to take due care of the computer and return it when requested.

Signed …………………………………… Date…………………………………

Appendix iii

Lakeside School

e-Safety Rules

- These e-Safety Rules help to protect students and the school by describing acceptable and unacceptable computer use
- The school owns the computer network and can set rules for its use
- It is a criminal offence to use a computer or network for a purpose not permitted by the school
- Irresponsible use may result in the loss of network or Internet access
- Network access must be made via the user's authorised account and password, which must not be given to any other person
- All network and Internet use must be appropriate to education
- Copyright and intellectual property rights must be respected
- Messages shall be written carefully and politely, particularly as e-mail could be forwarded to unintended readers
- Anonymous messages and chain letters are not permitted
- Users must take care not to reveal personal information through e-mail, personal publishing, blogs or messaging
- Use for personal gain, gambling, political activity, advertising or illegal purposes is not permitted

The school may exercise its right to monitor the use of the school's computer systems, including access to websites, the interception of email and the deletion of inappropriate materials where it believes unauthorised use of the school's computer system may be taking place, or the system may be being used for criminal purposes for storing unauthorised or unlawful text, imagery or sound.

Lakeside School

e-Safety Rules

All pupils use computer facilities including Internet access as an essential part of learning, as required by the National Curriculum. Both pupils and their parents/carers are asked to sign to show that the e-Safety Rules have been understood and agreed.

Pupil Name: Year Group:

Pupil's Agreement

- I have read and I understand the schools e-Safety Rules
- I will use the computer, network, mobile phones, Internet access and other new technologies in a responsible way at all times
- I know that network and Internet access may be monitored

Signed: Date:

Parent's Consent for Web Publication of work and photographs

I agree that my sons work may be electronically published. I also agree that appropriate Images and Video that include my son may be published subject to the school rule that photographs will not be accompanied by pupil names.

Parent's Consent for Internet Access

I have read and understood the school e-Safety Rules and give permission for my son to access the internet. I understand that the school will take all reasonable precautions to ensure the pupils cannot access inappropriate material but I also appreciate that this is a difficult task.

I understand that the school cannot be held responsible for the content of materials accessed through the Internet. I agree that the school is not liable for any damages arising from the use of Internet facilities.

Signed: Date:

Please print name: