# Acceptable Use Policy

This policy defines and describes the acceptable use of ICT (Information and Communications Technology) and mobile phones and devices for school-based employees, and other authorised users, e.g. suppliers, contractors, visitors and volunteers. Its purpose is to outline the standards that must be observed when using school ICT systems, minimise the risk to pupils of inappropriate contact from employees and adults working with children who have been given access to the School's IT network – herein referred to as 'Users'), to protect employees and schools from litigation and to minimise the risk to ICT systems.

This policy aims to:

- protect the good reputation of the School
- support and enable effective use of technology whilst protecting the School's data and IT systems from viruses and unauthorised access
- set out the key principles expected with respect to the use of technology
- assist adults working with children to work safely and responsibly with the Internet and other communication technologies and to monitor their own standards and practice
- set clear expectations of behaviour and codes of practice relevant to responsible use of the Internet for educational, personal or recreational use
- set clear structures to deal with online abuse, such as cyber-bullying, which are cross referenced with other School policies and ensure that everyone is aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken
- minimise the risk of misplaced or malicious allegations made against adults who work with pupils.

**School Responsibilities**

The Head and the School's Governing Body are responsible for ensuring that employees of the School act in a lawful manner, making appropriate use of School technologies for approved purposes only. They are responsible for adopting relevant policies and the Head is responsible for ensuring that the School adopts the policy and all users are aware of its contents.

The IT Department is responsible for maintaining an inventory of ICT assets (hardware and software), including any equipment issued to staff for personal use, such as an iPad or mobile phone/device.

If any member of the School Community has reason to believe that any ICT equipment has been misused, they should consult the Head without delay. The Head will agree an appropriate strategy for the investigation of the allegations. Incidents will be investigated in a timely manner in accordance with agreed procedures.

Users found to be in breach of this policy may be disciplined in accordance with the School's Disciplinary, Capability and Grievance Procedure or terms laid out within Service Agreements. In certain circumstances, breach of this policy may be considered gross misconduct resulting in termination of employment or termination of contracts between the School and Users. Users must report all suspected breaches of this policy to the Head.

Users and their managers are responsible for ensuring that adequate induction, training and support is undertaken to implement this policy.

By logging on to the School's network, users agree to abide by this Acceptable Use Policy and other policies that relate to the use of ICT.

All users are expected to act in a responsible, ethical and lawful manner. Users should uphold privacy and confidentiality, especially the privacy and confidentiality of School pupils, in accordance with the Data Protection Act 2018 and the School's Data Protection and Data Retention policies. The aforementioned policies are updated every two years, as a minimum. Care must also be taken not to breach another person's copyright, trademark or design, nor to publish any defamatory content.

Users provided with any mobile device, such as an iPad or mobile phone, sign for its use on receipt (see Appendix 1). Users may use School equipment for authorised business use only.

Users must follow authorised procedures when relocating ICT equipment or taking mobile devices offsite.

No one may use ICT resources in violation of license agreements, copyrights, contracts or national laws.

Portable ICT equipment is password protected with a minimum password of 6 characters. Users must update this password on a regular basis, as directed by the IT team.

Users of the ICT system, and / or ICT equipment, are required to protect and keep confidential their password and not share their account details with others for their use, nor utilise another users' account or misrepresent their identity for any reason. Users must not under any circumstances reveal their password to anyone else.

No user shall use (e.g. read, write, modify, delete, copy, move) another user's personal electronic documents (including email) without the owner's permission or as allowed by this policy or by law.

Users must not load or download software on any device without the authorisation of the line manager. Periodic audits of software held on ICT equipment will be undertaken.

Users must not download personal data (in particular, any data relating to pupils) from the School onto personal devices without authorisation from the Head. Electronic data is only accessible outside School, through the Cloud platforms including SharePoint and SchoolBase. Users must be particularly vigilant if they use the school's ICT equipment outside the workplace and take such precautions as we may require from time to time against importing viruses or compromising system security e.g encryption. The system contains information which is confidential and/or subject to data protection legislation. Such information must be treated with extreme care and in accordance with the School's Data Protection Policy.

Any device connecting to the School network must have School approved anti-virus software installed and activated. Users may not turn off anti-virus software. All users of ICT resources have the responsibility to take precautions to prevent the initial occurrence and subsequent spreading of a computer virus. Users may not knowingly create, install, run, or distribute any malicious code (e.g. viruses, Trojans, worms) or another destructive program on any ICT resource.

No one may knowingly or willingly interfere with the security mechanisms or integrity of ICT resources. No one may use ICT resources to attempt unauthorised use, or interfere with the legitimate use by authorised users, of other computers on internal or external networks. Access to networks will be monitored.

In accordance with data protection legislation, namely the Data Protection Act 2018, the Human Rights Act 1998, Regulation of Investigatory Powers Act 2000 and the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 as amended, extended or re-enacted from time to time, Lochinver House School may record or inspect any information transmitted through or stored in its computers, including e-mail communications and individual login sessions, without notice in certain circumstances including, but not limited to, the following:

- There is reasonable cause to believe the user has violated or is violating this policy, any guidelines or procedures established to implement this policy.
- An account appears to be engaged in unusual or unusually excessive activity.

- It is necessary to do so to protect the integrity, security, or functionality of ICT resources or to protect Lochinver House School from liability.
- Establishing the existence of facts relevant to the business.
- Ascertaining or demonstrating standards which ought to be achieved by those using the ICT facilities.
- Finding lost messages or to retrieve messages lost due to computer failure.
- Preventing or detecting crime.
- Investigating or detecting unauthorised use of ICT facilities.
- Ensuring effective operation of ICT facilities.
- Determining if communications are relevant to the business (for example, in the last resort where an employee is off sick or on holiday and business continuity is threatened).
- Permitted or required by law.

Email communication and any user data held on school equipment may be inspected by the IT Team with the authorisation of the Head for the reasons provided above. Other Internet based communication, such as web browsing, is monitored using automated software.

It is prohibited to send private, sensitive or confidential information by unencrypted email – particularly to an external recipient - as accidental disclosure could lead to significant harm or embarrassment. Personal data should be anonymised where possible. Passwords must be used on sensitive documents that must be sent to external recipients. The IT Team provide advice and guidance on email encryption solutions if this is required. Please also see the Data Protection Policy.

Websites should not be created on school equipment without the written permission of the Head.

No one may use ICT resources to transmit abusive, threatening, or harassing material, chain letters, spam, or communications prohibited by law, or may impact the image or reputation of the school. No one may abuse the policies of any newsgroups, mailing lists and other public forums through which they participate from a School account.

Users should adhere to the 'good practice guidelines for email communication', contained within the Online Safety Policy.

The following content must not be downloaded from, created or accessed on ICT equipment at any time:
- Pornographic material (that is, writing, pictures, film and video clips of a sexually explicit nature).
- Material that gratuitously displays images of violence, injury or death.
- Material that is likely to lead to the harassment of others.
- Online gambling.
- Junk email.
- Material that promotes intolerance and discrimination because of race, sex, disability, sexual orientation, religion or age.
- Material relating to criminal activity.
- Music or video files or other material in breach of copyright.
- Material that may generate security risks and encourage computer misuse.

It is possible to access or be directed to unacceptable Internet sites by accident. These can be embarrassing and such sites can be difficult to get out of. If users have accessed unacceptable content or are in receipt of unacceptable material via email, they must inform the Head or the Designated Safeguarding Lead and IT Support. This may avoid problems later should monitoring systems be alerted to the content.

If staff are are accessing their work Office 365 accounts on a personal device, they must ensure that their personal device has security and anti-virus software in place. When accessing school email, under no circumstances must the built-in mail app be used, users are required to use the Microsoft Outlook app or Microsoft's webmail platform. All users are reminded that forwarding school emails to personal accounts is prohibited. Cloud storage platforms must not be used for work purposes with the exception of the school managed OneDrive.

Users must not connect any personal ICT equipment (e.g. laptop, netbook) to the school network. Any requirement needs to be agreed and co-ordinated with the IT Department

All portable ICT equipment must be locked away or safely secured when not in use. Any user authorised to use portable equipment, such as a laptop, for home or roaming use must take all reasonable efforts to keep the equipment safe and secure.

For security purposes users must log off or lock their computer at all times when they step away from their desk. Users must shutdown their computer at the end of the day.

Users must not copy or install school software to any personal equipment without authorisation from the Head.

Digital recording equipment e.g. cameras may be available for users to use as part of delivering ICT and the broader curriculum. Safe and appropriate use of recording equipment must be discussed with the pupils as part of the curriculum and referred to whenever recording is to take place.

Users must not use images and recordings for activities and purposes beyond school endorsed projects. The materials are not to be circulated in the public domain and are not to be used for personal gain.

Users issued with a lochinverhouse.com email address must not use this email address to make orders for personal goods and services or to sell personal goods and services or to sign up for any personal services (except those expressly authorised by SLT). Likewise, if a user wishes to make a complaint to the third-party supplier or manufacturer about personal goods or services received, the lochinverhouse.com e-mail address must never be used under any circumstances. These are entirely personal transactions and so users must not hold themselves out as acting for or on behalf of Lochinver House School or must not in any way indicate that the transaction is connected to the School.

**Mobile Phone Communication and Instant Messaging**

All online activity, both in and outside School, will not bring the School, your or anyone's professional reputation into disrepute.

- Users must not give their home telephone number or their personal mobile phone number to pupils. Mobile phone communication should be used sparingly and only when deemed necessary.
- Photographs and videos of pupils must not be taken with personal mobile phones or any other personal device. Photographs must only be taken on school devices, for approved school business
- Staff should only communicate electronically with pupils from School accounts on approved School business, e.g. class work.
- Users should not enter into online messaging communications with pupils other than via the school and ICT System and for approved school business.
- Users should not make use personal mobile devices in the presence of School pupils. For those working with or supporting in the EYFS, the 'Use of Mobile Devices in the EYFS' policy must be adhered to.

**Social Networking Sites**

The School successfully runs a number of social networking pages as a marketing tool. The School has administrative rights over the accounts, monitoring them regularly to ensure the content enhances the School's reputation.

- Users must not communicate or connect with any current pupil or former pupil under the age of 18 on any personal social networking site without the written permission of the Head.
- Users should not create any social networking group that links directly to the School without the written permission of the Head.
- Users should not use social networking sites to discuss work related issues or to use their position at the school to further their own interests.
- Users should only communicate electronically with pupils from school social networking accounts on approved School business, e.g. School events.

- If users have a social networking profile that is either 'open' or 'semi-closed', pupils are likely to come across it. Users should model appropriate behaviour or make profiles completely unavailable to those to whom access has been refused.

**Promoting Online Safety**

The School takes Online Safety education very seriously and has taken steps to ensure that pupils, parents and users receive clear guidance on the safe use of technology. Upon joining the School, all parents are given access to the Online Safety Policy. All pupils are required to sign the Online Safety Agreement.

- Online Safety is taught to all pupils through their computing lessons, the PSHE curriculum and through visiting speakers.
- The Head of Computing & Digital Learning has undertaken CEOP Ambassador training with the Child Exploitation and Online Protection Service. The training resources are shared with users and used for teaching the PSHE and Computing curricula.
- The School takes the view that pupils should be prepared for the challenges of the digital world and to be digitally resilient as well as appreciating the benefits of such technology.
- Pupils are taught how to use social media responsibly, how to report concerns and given guidance on how to recognise when they may be in danger.
- Pupils are taught that exposure to misinformation and disinformation, including false or misleading content that can distort their understanding of current events, health, or social issues.
- Pupils are taught that engagement with conspiracy theories and other forms of online manipulation that may influence beliefs or behaviours in harmful ways.
- Pupils are taught about harmful online conduct, such as peer pressure to participate in risky challenges, oversharing personal information, or engaging in trolling or harassment.
- Pupils are taught about the risks associated with online commerce, including scams, exploitation through in-game purchases, and exposure to advertising that targets children inappropriately
- The School has an online resource 'The Sharp System' which enables pupils in Year 3 and above access to report any type of bullying or concerns, including those related to cyber-bullying and Online Safety.
- The School's website contains relevant and up-to-date information for parents regarding Online Safety.
- Online Safety is everybody's responsibility and everyone is responsible for promoting positive Online Safety messages at all times.

**Artificial Intelligence (AI)**

The school acknowledges the significant benefits of AI in an educational context, including enhancing teaching and learning, improving outcomes, streamlining administrative processes, reducing workload and preparing staff and learners for a future in which AI will be integral. AI tools should be used to promote learning, creativity and fairness, while avoiding misuse such as plagiarism or the creation of harmful content. Staff are encouraged to use AI-based tools to support their work where appropriate, within the frameworks provided below, and are expected to exercise professional responsibility and accountability in this area. Please refer to the AI Policy for further information about AI.

| | |
|---|---|
| Reviewed By | Head of Computing |
| Approval Body/ Committee | Education |
| Last Review | Autumn 2026 |
| Next Review | Autumn 2027 |
| Policy Linked To | AI Policy, Anti-Bullying Strategy, Behaviour Policy, Child Protection and Safeguarding Policy (incorporating Staff Behaviour and Code of Conduct), Data Protection Policy, Health and Safety Policy, Online Safety Policy, Privacy Notice, Personal, Social, Health and Education (PSHE) Policy, Remote Learning Policy, Spiritual, Moral and Cultural (SMSC) Policy, Use of Mobile Devices in Early Years Foundation Stage Policy. |

*Any data held in relation to the content of this policy will be managed in accordance with our Data Protection Policy and Privacy Notice.*

## Appendix 1 - School Devices Agreement

**Terms:**

- All School devices (iPads, mobiles, laptops) remain the property of Lochinver House School.
- You will comply at all times with the School's Online Safety Policy and Acceptable Use Policy. Failure to comply could result in disciplinary proceedings.
- Your right to use and possess the device is determined by your position in the School and will terminate:
    - if your position changes and the device is no longer needed
    - if the requirements of your role change and the device is no longer needed; or
    - on your last day of employment at the School.
- The vast majority of updates will be deployed to the devices remotely; however, the School may occasionally recall the devices to install essential updates. You must hand in your device for this purpose when requested.
- The School makes every effort to block inappropriate websites and content both inside and outside of School by installing a filtered browser on each device. Using software utilities or other means to access blocked content is a breach of the Acceptable Use Policy and could result in disciplinary action.
- Any personal use on a School device must comply with the Online Safety Policy and Acceptable Use Policy.
- Inappropriate content is not allowed on School devices and the presence of such materials will result in disciplinary action.
- School devices will have security applications installed. Deletion of security-related apps is prohibited and a breach of the School's Acceptable Use Policy.
- Your Apple ID is managed by Lochinver House School. If you require an app to support teaching and learning, please email IT Support with your request with at least 48 hours notice.The School device comes equipped with a microphone, front and rear-facing camera, and video capability. Lochinver House School retains the rights concerning any image or recording.
- You must obtain permission from a member of the School's SLT before publishing an image or recording of any School-related activity. Unauthorised images and recordings are subject to disciplinary action in accordance with the School's Acceptable Use Policy.
- Your School device should be protected with a suitably complex passcode at all times. This passcode should be known only by you to ensure the device is only used by you. Lochinver House School retains the right to bypass the passcode.
- You may not lend your device to anyone or borrow another user's device. Access to another person's account or device without consent or knowledge is considered hacking and is prohibited in accordance with School's Acceptable Use Policy.
- You must not lend your device to a pupil.
- Your device should not be modified in any way that will permanently alter it, either physically and/or electronically, other than instructed by a member of the SLT or IT team.
- You should not remove the device's case. Repairs to any damage caused by the case being removed will be deducted from your salary via the monthly payroll.

**Loss, Theft or Damage**

Due to the excess on the School's insurance policy (which means that the School is in effect self-insuring School devices), please note that if one or more of the following events should happen on three or more occasions, you will be liable for any repair or replacement costs which will be deducted from your salary via the monthly payroll:

- you lose your device or any associated charging cables/adaptors/case
- your device or any associated charging cables/adaptors/case is stolen from a vehicle or unsecured premises
- your device or any associated charging cables/adaptors/case is damaged (accidentally or otherwise)
- your device or any associated charging cables/adaptors/case malfunctions and it is established that your actions or inactions have resulted in that malfunction.

For the avoidance of any doubt, if the device (or any associated charging cables/adaptors/case) malfunctions and it is not as a result of your actions or inactions, then you will not be liable for any repair or replacement costs. Similarly, if the device (or any associated charging cables/adaptors/case) is stolen from your secured home or whilst in your possession, then you will not be liable for any repair or replacement costs.

You may forfeit your right to retain use of a School device if the device is repeatedly damaged or lost or you have not followed the agreements set out here.

Please sign the attached form and return to our HR Department.

**User agreement**

I confirm that I have read and understood the School Devices Agreement.

I confirm that I have read and understood the School's Online Safety Policy and Acceptable User Policy.

I agree to follow the School's policies regarding the use of School devices.

I agree that the School can deduct monies from my salary via the monthly payroll to pay for any repair or replacement costs arising from loss, theft or damage to the device.

| | |
|---|---|
| Name | |
| Job title | |
| Signed | |
| Date | |