ACCEPTABLE USE OF IT POLICY FOR SENIOR SCHOOL PUPILS

Owner: **DMP**
Reviewed: **March 2026**
Next Review: **March 2027**

The computer system is owned by the School and may be used by you as part of your education. All computer-based activity should be appropriate to a school environment. This Policy has been drawn up to protect the interests of the School, staff and all pupils, including you. The internet provides a wealth of information, allowing users with appropriate software to access and exchange text, graphics, sound and video-based information. Access to the internet is provided for every pupil. Digital awareness, including staying safe online, is covered in School assemblies, Computing lessons, Life Advice sessions and Form Times for pupils and parents.

The School reserves the right to examine or delete any files held on the School's system (including the School's 365 cloud storage) and to monitor both files held, and internet sites visited; at all times when visiting an internet site your identity (which is linked to the School's) may be logged; this includes using mobile devices connected to the School Wi-Fi. All material held on the School network remains the intellectual property of the School.

GUIDELINES FOR THE USE OF THE SCHOOL NETWORK

You agree to the following guidelines for use of the School network (whether on School iPads or personal devices):

- During lesson time you may only use your school iPads (or the designated BYOD in sixth form). Personal mobile devices are not for use in lessons and should not be used to access the internet. Below sixth form, mobile phones should be kept in their Yondr pouch between registration and 4pm. Sixth form pupils must only use their mobile phones in the common room or outside.
- You must not attempt to bypass the School's security controls or internet filtering by using mobile hotspots, mobile tethering, unauthorized VPN or any other method.
- Mobiles or iPads will be confiscated and examined if it is considered they are being used in contravention of any aspect of this Policy.
- Computers in the Computing rooms, LRC and common rooms are to be used only for academic work.
- You may not log on to desktop computers in classrooms or access the interactive whiteboards, Apple TV or Native Airplay using your own devices outside lesson times or without the permission of a teacher.
- LEHS WiFi should only be used for school iPads during school hours. Sixth formers should use the BYOD WiFi for any BYOD Laptop or other personal devices.

Passwords

- Access should only be made via your authorised username and password, which should not be made available to any other person. You must not log on to someone else's account. You must log off or lock your computer or iPad when it is unattended.
- For security reasons, you are required to change your password every 180 days using a complex password. An email will be sent 5 days before your password is due to expire. Passwords must be changed when requested or if your password is known by someone else. Passwords should not be obvious, and nor should they be the same for any password you use to access your personal devices. If you are aware of another person's password, you should inform them straight away.

Filtering

- Internet use is for schoolwork or email only. The School will take all reasonable precautions to ensure that users access only appropriate material. All material available, including websites accessed by a secure connection, will be filtered by our internal filter. IT Services have the ability to track and monitor your internet use and will be automatically alerted should an inappropriate search be carried out.
- We aim to ensure that you are not at risk of radicalisation through access to extremist material and aim to ensure that you have no access to any material or images that are not suitable. It is not possible, however, to guarantee that particular types of material will never appear on a terminal, given the international scale and linked nature of information stored on the internet. It is the responsibility of individual users to ensure that the internet is used appropriately for schoolwork. This includes internet access from mobile devices using the School Wi-Fi. If you have any concerns about what you see on the internet, you should speak to the Digital Leader for Student Training or the Deputy Head (Pastoral) immediately.
- If a virus is detected by the anti-virus software, you must immediately inform the Director of Information Systems or email itsupport@lehs.org.uk.

Use of Email

- Emails should only be sent to those you know, or as directed by your teachers. Usage is monitored and abnormal use will be investigated. Ensure your online communications are (and anything you share online is) appropriate, respectful and composed in a way you would stand by. Sending threatening, abusive or embarrassing messages or forwarding chain letters is forbidden.
- Emails should not be sent during lessons unless directed by your teacher.
- Emails sent on official School business (e.g. arranging Work Experience) should be checked by the teacher before being sent.
- Confidential information must not be sent via email. Personal information or credit card details must not be given on the internet. No goods or services may be ordered.
- Emails will automatically be labelled as from LEH. Any other email services may not be used on the School computers.

Use of Microsoft Teams

- Pupils must not use Microsoft Teams to call any member of staff.
- Microsoft Teams communications should be appropriate, respectful and composed in a way you would stand by. Sending threatening, abusive or embarrassing messages is forbidden.
- Pupils may communicate with their teachers by posting messages in the class team, using the @ function to mention the teacher. All online communication should be appropriate and respectful at all times. Pupils should use a new post rather than one associated with a lesson to prevent other pupils being disturbed by notifications.
- The Microsoft Teams communication functions should not be used in a lesson unless you have been given permission by a member of staff.
- When using Teams for remote lessons please comply with the Guidance for Remote Lessons and the Remote and Hybrid Teaching Policy.

SENIOR SCHOOL GUIDELINES FOR PUPILS' RESPONSIBLE USE OF SCHOOL IPADS

You agree to use the School iPads in accordance with the following guidelines:

- All pupils in 3rds to U5 must have a working iPad and active stylus. (See appendix for sixth formers on BYOD)
- You must bring your iPad to School every day with sufficient charge. Create a routine of plugging your iPad in and connecting it to Wi-Fi overnight, next to your School bag. This will ensure that it has sufficient charge for the School day and that your data is backed up to the cloud. iPads may not be charged in School.
- It is your responsibility to ensure the iPad is working at all times. This includes updates to the latest iPadOS version when instructed. You should contact IT Services if there is an issue.
- iPads may only be used in lessons and classrooms with the express permission of your teachers. Only content or apps that are relevant to the lesson should be accessed. iPads should be closed at all other times. Authorised apps are downloadable from the Self Service app. Should pupils or parents have any issues with any apps, please raise them with your Form Tutor or IT Services.
- Do not use your device in School corridors or other unauthorised areas. Middle School pupils must not use iPads during lunchtime. If homework for any reason needs to be done at lunchtime using an iPad, this can be done only in the LRC.
- If you misplace your iPad in school, you must let IT Services know immediately so that its general location might be identified. This is only possible if it is connected to the School Wi-Fi and the battery has charge left.

Storage and Security

- The iPad must remain in your possession, should only be used by you and should be securely stored when not in use.
- The iPad must be clearly labelled with your name and form, remain in its protective case at all times and have a PIN (or more secure password) set on it which is used at all times. This must be changed if it becomes known by others.
- The iPad must have Location Services enabled.
- If the iPad is damaged, an insurance claim must be made as soon as possible. This does not cover the accidental loss of the iPad. The information about how to file an insurance claim is

on the Parent Portal and is to be completed by your parents. This does not apply if you have opted out of the insurance.

- Your Apple Pencil is not traceable. You must, therefore, ensure that it is clearly labelled with your name and that you keep the box which has a record of the serial number. You should store your Apple Pencil in the iPad case whenever it is not being used.

Backup and Apps

- Backup of content on the iPad, either to iTunes or iCloud, is your responsibility. You should complete all work in your school OneDrive so that you can ensure your work is recoverable.
- Apps on the 'blacklist' must not be on the iPad. The 'blacklist' will be made available on SharePoint and the Parent Portal.
- Age limits on apps, including for social media apps, must be adhered to. You should not be using these sites below the stipulated ages, even at home.
- We reserve the right to ask for the removal of any app not approved by the School.
- Pupils in 3rds-U5 will not have access to the Apple App Store and can only download apps via the Self Service app. The School reserves the right to review which other year groups (and individual pupils) have access to the Apple App Store from time to time.
- If you enable notifications on apps installed on your iPad, ensure that these are silent to avoid disruption to lessons.

USE OF SCHOOL INTERACTIVE BOARDS AND SPEAKERS

These exist for learning purposes only. You may not use a staff computer or the interactive boards or speakers without the presence and permission of a member of staff.

SOCIAL MEDIA USE / ONLINE CONNECTED SERVICES

You agree to use social media/online connected services in accordance with the following guidelines:

- Information, images, video or any other material which could be illegal or cause offence or embarrassment to you, other members of the School community or anyone else should not be published on any website or online service (e.g., Facebook, Twitter, ASKfm, Tellonym, Blogspot, Tumblr, Instagram, SnapChat, WhatsApp, TikTok).
- You will not use digital technology of any sort to bully/victimise members of the School community or anyone else. Incidents of cyberbullying should be reported as soon as possible to a Form Tutor, Head of Year, Head of Section, Deputy Head (Pastoral) or the Digital Lead, Student Training. All reports will be taken very seriously. The School will react quickly to all incidents in accordance with its Anti-Bullying Policies.
- You may follow the official school Twitter or Facebook accounts. You must not add or follow individual teachers or other staff members on social media. You may not record and store images or videos of staff on your iPad or any other device.
- You must not share personal details (names, photos etc.) of LEH pupils or members of staff online without their permission, including tagging them in photos on social media.
- You should follow the advice given to you in Computing lessons, Life Advice lessons and talks on the safe and productive use of social media and the internet.

USE OF ARTIFICIAL INTELLIGENCE (AI)

You agree to use artificial intelligence programs in accordance with the following guidelines:

- Teachers will clarify where AI can be used and how extensively. You must ask your teacher if you require further clarification or have questions BEFORE using AI for any assignment.
- You may use age appropriate Generative AI where your teachers have indicated it suitable. However, you should note that the material generated by these programs may be inaccurate, incomplete, or otherwise problematic. You must check and verify ideas and answers against reputable source materials.
- Large language models (LLMs) can make up incorrect facts and fake citations. Code generation models can produce inaccurate outputs. Image generation models can produce biased or offensive products. You are responsible for any content you submit, regardless of whether it originally comes from you or a foundation model.
- You should not use AI tools to ask questions about health / medical / wellbeing issues, or indeed anything of a personal nature. It is always best to seek help and recommendations as to reliable resources from a member of staff.
- You should always adhere to the age restrictions for different LLMs. For instance, ChatGPT has a 13+ restriction (Is ChatGPT safe for all ages? | OpenAI Help Center).
- You should not enter personal or confidential information into generative AI tools. This technology stores and learns from data inputted and you should consider that any information entered into such tools (including original content you create) is released to the internet.
- (*If you are, or will, turn 18 during this academic year*), you agree that any data or content you create which is inputted into generative AI tools, whether by you or by a teacher, may be used by those tools to train their models; this includes any intellectual property you may own in respect of original content you create.
- You agree that personal data (such as your name and username) may be shared and used to create an account with any AI powered educational platforms your teachers use to support teaching and learning.
- You must indicate what part of the assignment was written or created by AI and what was written or created by you. You may not submit any work generated by an AI program as your own.
- The submission of AI-generated answers without appropriate citation constitutes plagiarism and is a breach of the School's pupil code of conduct. The school uses Turnitin to identify possible instances of unacknowledged use of AI.

For further information about AI see the AI policy.

DATA PROTECTION

The School has an obligation to keep all personal information (names, email addresses, opinions on a person) relating to all individuals: pupils, parents, staff etc. secure. This means personal information should not be shared with others more than is necessary and the School needs to ensure its IT systems remain as secure as possible, so personal information is not lost. Pupils have a part to play in keeping information held by the School secure:

- If you lose your iPad, you must inform IT Services immediately in order that they can consider what personal information may have been lost or is at risk of being lost.
- Be vigilant and do not open emails if it is not clear as to who/where they are from (in particular on iPads where full sender details may not be visible due to the small screen) and inform IT Services immediately.
- Double check email addresses before sending to ensure emails are sent to the correct recipients, especially due to autofill. Avoid the use of reply all.
- Respect other people's privacy and do not share information where it is clearly marked as confidential or people's details e.g., email addresses without their consent. Seek permission from any staff or pupils of whom you intend to take pictures or videos. Additional consent will also be required if you intend to use the content online.

PARENTAL RESPONSIBILITY

Technical barriers can never entirely protect a child from harmful online content. Parents should be aware that whilst the School's IT facilities are implemented in such a way as to support a safe and secure environment in which to learn, the same protection is not in place when using other networks, including those at home. Although our use of Yondr pouches for 3rds to U5 limit pupil access, smart phones usually have an internet connection through data roaming (4G/5G) which does not have any content filtering in place and can be used to access any material on the internet. It is strongly recommended that any 4G/5G account for pupils be requested with a teenage filter for safe internet access outside of the School.

Whilst the School takes the actions described above to ensure that pupils understand the importance of safe behaviour online, the School cannot be held responsible for inappropriate online behaviour that bypasses the School network (which can occur whilst using mobile data and some apps, even whilst used on School site).

In light of this, parents must also be responsible for ensuring that their child uses technology in a safe and secure way and that their child behaves responsibly when online. It is recommended that parents have appropriate controls on their Wi-Fi at home as the School's filtering service, Smoothwall, only works when pupils are in school. The full range of School sanctions will be considered in the event of any breach of this Policy in accordance with the School Rules.

Both the School and parents have a responsibility to ensure that pupils have the knowledge and confidence to know what to do if they encounter content or receive communications that make them feel uncomfortable, worried or upset and are able to share their concerns in an open and supportive environment. For pupils, this is addressed in the curriculum through Life Advice and Computing lessons, pastorally in form time and through the Sixth Form Digital Mentors under the auspices of the Digital Leader for Student Training, The Digital Leader for Student Training shares information and updates periodically via the Friday Post or School Post.

RELATED POLICIES

Remote and Hybrid Teaching Policy
AI Policy
Policy to Promote Good Behaviour
Anti-Bullying Guidelines

APPENDIX 1 BRING YOUR OWN DEVICE (SIXTH FORMERS ONLY)

Sixth Form pupils have the choice to bring in a laptop in place of the school iPad. This must adhere to the following criteria:

- The device is compliant with the school systems. This means that it must be running a supported and fully updated version of Windows 10, Windows 11 or macOS. In the case of macOS, it must have anti-virus software installed too. Chromebooks are not compatible with our systems and cannot be used as a BYOD.
- Each student must still have the facility for digital writing. This means that students should either have a laptop with a touch screen/writing function, or they will need to retain their old iPad and stylus or purchase a Graphic Tablet. The digital writing function of iPads continues to be employed widely, especially with the use of OneNote, and is an embedded use within subjects (such as Maths A-Level).
- The device must have a battery life that allows it to be used through the school day without needing to be charged. Pupils must ensure that their device has the necessary battery life for the day before they arrive in school.
- The device must be able to install Microsoft 365 products.
- The device will need to be registered on our 'LEH BYOD' Wi-Fi network in school.
- Pupils will be expected to maintain these devices themselves, updating operating systems and sorting out issues. IT Services can be contacted to deal with problems getting onto the network, downloading MS 365 Apps etc., however, they are not there to solve hardware or additional software problems.
- The 'LEH BYOD' Wi-Fi network provides access to the internet only. No other access to systems (e.g. printing) is available. Printing remains available on school computers provided at various locations in the school.
- Pupils must follow the same guidelines on appropriate use as laid out in this document.