THE HOSPITAL SCHOOL AT GREAT ORMOND STREET & UCLH

ICT Acceptable Use Policy

The Hospital School at Great Ormond Street & UCLH		
Review Frequency	Two years	*Next review date: Autumn 2026*
Previous Reviews	HT internal review October 2021	
Full Governing Body Ratification	FGB	*Date: 10.10.24*
Approving Committee	N/A	*Date: N/A*
Policy Holders (name of staff)	Headteacher	

Table of Contents

1. Introduction and aims

Information and communications technology (ICT) is an integral part of the way our school works, and is a critical resource for pupils, staff, governors, volunteers and visitors. It supports teaching and learning, pastoral and administrative functions of the school.

However, the ICT resources and facilities our school uses also pose risks to data protection, online safety and safeguarding.

This policy aims to:

- Set guidelines and rules on the use of school ICT resources for staff, pupils, parents and governors
- Establish clear expectations for the way all members of the school community engage with each other online
- Support the school's policy on data protection, online safety and safeguarding
- Prevent disruption to the school through the misuse, or attempted misuse, of ICT systems
- Support the school in teaching pupils safe and effective internet and ICT use

This policy covers all users of our school's ICT facilities, including governors, staff, pupils, volunteers, contractors and visitors.

Staff should also refer to the staff laptop agreement and school's online safety policy which can be found in Google Drive ->Staff->Policies -> Current Policies ALL.

Breaches of this policy may lead to loss of access to and use of School facilities and further action (including disciplinary and/or criminal proceedings).

2. Definitions

- **"ICT facilities":** includes all facilities, systems and services including but not limited to network infrastructure, desktop computers, laptops, tablets, phones, cameras, or hardware, software, websites, web applications or services, and any device system or service which may become available in the future which is provided as part of the ICT service
- **"Users":** anyone authorised by the school to use the ICT facilities, including governors, staff, pupils, volunteers, contractors and visitors
- **"Personal use":** any use or activity not directly related to the users' employment, study or purpose
- **"Authorised personnel":** employees authorised by the school to perform systems administration and/or monitoring of the ICT facilities
- **"Materials":** files and data created using the ICT facilities including but not limited to documents, photos, audio, video, printed output, web pages, social networking sites and blogs

3. Unacceptable use

The following is considered unacceptable use of the school's ICT facilities by any member of the school community.

Unacceptable use of the school's ICT facilities includes:

- Using the school's ICT facilities to breach intellectual property rights or copyright
- Using the school's ICT facilities to bully or harass someone else, or to promote unlawful discrimination
- Breaching the school's policies or procedures
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Online gambling, inappropriate advertising, phishing and/or financial scams
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate or harmful
- Consensual and non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams (also known as sexting or youth-produced sexual imagery)
- Activity which defames or disparages the school, or risks bringing the school into disrepute
- Sharing confidential information about the school, its pupils, or other members of the school community
- Connecting any device to the school's ICT network without approval from authorised personnel
- Setting up any software, applications or web services on the school's network, computer or laptop without approval by authorised personnel, or creating or using any program, tool or item of software designed to interfere with the functioning of the ICT facilities, accounts or data
- Gaining, or attempting to gain, access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel
- Allowing, encouraging or enabling others to gain (or attempt to gain) unauthorised access to the school's ICT facilities
- Causing intentional damage to ICT facilities
- Removing, deleting or disposing of ICT equipment, systems, programs or information without permission by authorised personnel
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation
- Using inappropriate or offensive language
- Promoting a private business, unless that business is directly related to the school
- Using websites or mechanisms to bypass the school's filtering mechanisms
- Engaging in content or conduct that is radicalised, extremist, racist or discriminatory in any other way

This is not an exhaustive list. The school reserves the right to amend this list at any time. The headteacher will use professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of the school's ICT facilities.

3.1 Exceptions from unacceptable use

Where the use of school ICT facilities (on the school premises and/or remotely) is required for a purpose that would otherwise be considered an unacceptable use, exemptions to the policy may be granted at the headteacher's discretion.

4. Staff (including governors, volunteers, and contractors)

4.1 Access to school ICT facilities and materials

The school's ICT support team (Crossover Solutions) and the Assistant Head (Learning Technology) jointly manage access to the school's ICT facilities and materials for school staff. That includes, but is not limited to:

- Computers, tablets, mobile phones, VR headsets, cameras and other devices
- Access permissions for certain programs or files

Staff will be provided with unique log-in/account information and passwords that they must use when accessing the school's ICT facilities.

Staff who have access to files they are not authorised to view or edit, or who need their access permissions updated or changed, should contact the Assistant Head (Learning Technology) or Crossover Solutions. If issues cannot be resolved on site, a call will be raised with Crossover Solutions and they will aim to resolve these issues within their Service Level Agreement (SLA).

The School reserves the right to monitor Internet and network use and activity and examine and delete files and folders from the School's systems, as required.

During School hours, staff should only access work related Internet sites via the LGfL Internet connection. Access to personal email accounts, non-work related web sites, social networking sites and blogs is not allowed. Failure to comply may result in disciplinary action being taken.

Users should always log out of systems and lock their equipment when they are not in use to avoid any unauthorised access. Equipment and systems should always be logged out of and shut down completely at the end of each working day.

4.1.1 Use of phones and email

The school provides each member of staff with an email address.

This email account should be used for work purposes only. E-mails and other online communications must be carefully written and polite in tone and nature.

All work-related business should be conducted using the email address the school has provided. Confidential data involving pupils can be sent between colleagues with secure NHS or LGFL email addresses e.g. @gosh.nhs.uk / @uclh.nhs.uk / @gosh.camden.sch.uk. When sending sensitive or confidential to other agencies e.g. home schools, any attachments containing sensitive or confidential information should be password protected so that the information is only accessible by the intended recipient.

First and last name combinations combined with any other identifying information (e.g. address, telephone number) should not be used in emails to identify a pupil.

Staff must not share their personal email addresses with parents and pupils, and must not send any work-related materials using their personal email account.

Staff must take care with the content of all email messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract.

Email messages are required to be disclosed in legal proceedings or in response to requests from individuals under the Data Protection Act 2018 in the same way as paper documents. Deletion from a user's inbox does not mean that an email cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable.

Where pupil data is taken off site, via staff laptops, tablets, USB sticks etc. the information must always be password protected and encrypted.

If staff receive an email in error, the sender should be informed and the email deleted. If the email contains sensitive or confidential information, the user must not make use of that information or disclose that information.

If staff send an email in error that contains the personal information of another person, they must inform the Assistant Head (Learning Technology) immediately.

Staff must not give their personal phone numbers to parents or pupils. Staff must use office phones or work mobile phones provided in the school to conduct all work-related business.

School office phones and work mobile phones must not be used for personal matters.

Staff who are provided with work mobile phones as equipment for their role must abide by the same rules for ICT acceptable use as set out in section 3.

Sharing and the use of other people's log-ins and passwords is not allowed. Users should always ensure that they log-out or use the "lock screen" feature when they leave a laptop/device unattended.

Files stored on School devices should be archived to Google Drive or deleted if no longer needed. The School reserves the right to delete 'old' files if necessary.

The school can record video meetings e.g. Zoom and Teams. If you record video meetings, callers **must** be made aware that the conversation is being recorded and the reasons for doing so. When on the call, inform them that you will be taking notes and also let them know if you will share these at the end of the meeting.

4.1.2 Use of Artificial Intelligence tools

Staff are advised to exercise caution and professionalism when using Artificial Intelligence (AI) tools, such as ChatGPT, Teachmate and Gemini. Staff should also be aware that AI tools are integrated into many existing software such as Adobe Photoshop and Google Search. AI-generated content must be reviewed for accuracy and appropriateness before use, as it may contain incorrect, biased, or inappropriate information. Staff must not input sensitive, personal, or confidential information into AI tools and should ensure that their usage complies with the school's online safety and safeguarding policies. Staff should use AI as a support tool rather than a sole source of information or decision-making.

4.2 Personal use

Any device (laptop, tablet, mobile phone) allocated by the school to individual staff is to be used within School to support teaching and learning and should wherever possible remain in school unless needed to work from home or to use for school related work at home as long as that work is reasonable, ethical and legal.

Staff are permitted to occasionally use school ICT facilities for personal use subject to certain conditions set out below. Personal use of ICT facilities must not be overused or abused. The Headteacher, Assistant Head (Learning Technology) or Crossover Solutions may withdraw permission for it at any time or restrict access at their discretion.

Personal use is permitted provided that such use:

- Does not take place during teaching hours
- Does not constitute ‘unacceptable use’, as defined in section 3
- Takes place when no pupils are present
- Does not interfere with their jobs, or prevent other staff or pupils from using the facilities for work or educational purposes

Staff may not use the school’s ICT facilities to store personal non-work-related information or materials (such as music, videos or photos).

Staff should be aware that use of the school’s ICT facilities for personal use may put personal communications within the scope of the school’s ICT monitoring software (see section 4.5). Where breaches of this policy are found, disciplinary action may be taken.

Staff are also permitted to use their personal devices (such as mobile phones or tablets) in line with the school’s online safety policy.

Staff should be aware that personal use of ICT (even when not using school ICT facilities) can impact on their employment by, for instance, putting personal details in the public domain, where pupils and parents could see them.

Staff should take care to follow the school’s guidelines on social media (see appendix 1) and use of email (see section 4.1.1) to protect themselves online and avoid compromising their professional integrity.

Staff should not allow School equipment or systems to be used or accessed by unauthorised persons and should keep any computers used at home safe and secure. Any theft or damage should be reported immediately to the School’s Business Manager. A police crime reference number will be required in the event of any theft.

Use of ICT facilities for personal financial gain, gambling, political purposes or advertising is not permitted at any time.

4.2.1 Personal social media accounts

Members of staff should ensure their use of social media, either for work or personal purposes, is appropriate at all times.

The school has guidelines for staff on appropriate security settings for Facebook and Instagram accounts (see appendix 1).

4.3 Remote access

We allow staff to access the school’s ICT facilities and materials remotely. Remote access is managed by Crossover Solutions and requires the Cisco AnyConnect app to be installed onto the laptop.

Staff will use their LGFL username and password to access the school drives remotely. Staff accessing the school’s ICT facilities and materials remotely must abide by the same rules as those accessing the facilities and materials on-site. Staff must be particularly vigilant if they use the school’s ICT facilities outside the school and take precautions against importing viruses or compromising system security.

Our ICT facilities contain information which is confidential and/or subject to data protection legislation. Such information must be treated with extreme care and in accordance with our data protection policy. This can be found on Google Drive ->Staff->Policies -> Current Policies ALL.

4.4 School social media accounts

The school has an official Instagram page (https://www.instagram.com/Gosh_school/) , managed by the Deputy Head (Curriculum Delivery) and Assistant Head (Teaching and Learning). Staff members who have not been authorised to manage, or post to, the account, must not access, or attempt to access the account.

The school has guidelines for what can and cannot be posted on its social media accounts. Those who are authorised to manage the account must ensure they abide by these guidelines at all times.

4.5 Monitoring of school network and use of ICT facilities

The school reserves the right to monitor the use of its ICT facilities and network. This includes, but is not limited to, monitoring of:

- Internet sites visited
- Bandwidth usage
- Email accounts
- User activity/access logs
- Any other electronic communications

Only authorised ICT staff may inspect, monitor, intercept, assess, record and disclose the above, to the extent permitted by law.

The school monitors ICT use in order to:

- Keep children safe while they are being educated at the school
- Obtain information related to school business
- Investigate compliance with school policies, procedures and standards
- Ensure effective school and ICT operation
- Conduct training or quality control exercises
- Prevent or detect crime
- Comply with a subject access request, Freedom of Information Act request, or any other legal obligation

5. Pupils

5.1 Access to ICT facilities

Computers and equipment in the school's classrooms are available to pupils only under the supervision of staff.

Chromebooks may be loaned to pupils to access work from their home school or to join a session remotely while they are self-isolating. Parents must sign a Chromebook loan form which should be returned to the Assistant Head (Learning technology).

Pupils will be provided with an account linked to the school's virtual learning environment (Google Workspace), which they can access from any device.

Staff have a responsibility to safeguard pupils in their use of the Internet and report all online safety concerns to a designated safeguarding lead or a deputy designated safeguarding lead.

6. Parents

6.1 Access to ICT facilities and materials

Parents do not have access to the school's ICT facilities as a matter of course.

However, parents working for, or with the school in an official capacity (for instance, as a volunteer or as a parent governor) may be granted an appropriate level of access, or be permitted to use the school's facilities at the headteacher's discretion.

Where parents are granted access in this way, they must abide by this policy.

7. Data security

The school is responsible for making sure it has the appropriate level of security protection and procedures in place. It therefore takes steps to protect the security of its computing resources, data and user accounts. However, the school cannot guarantee security. Users of the school's ICT facilities should use safe computing practices at all times.

7.1 Passwords

All users of the school's ICT facilities should set strong passwords for their accounts and keep these passwords secure.

Users are responsible for the security of their passwords and accounts, and for setting permissions for accounts and files they control.

Members of staff or pupils who disclose account or password information may face disciplinary action. Parents or volunteers who disclose account or password information may have their access rights revoked.

If you have forgotten the password to Google Workspace, this can be reset by the Assistant Head (Learning Technology). Any NHS passwords e.g. GOSH Gold and GOSH network can be reset by calling GOSH IT services on Ext. 6060. Please ask for a call reference number. Any other passwords are reset by Crossover solutions. Please email: support@crossover.solutions

7.2 Software updates, firewalls and anti-virus software

All of the school's ICT devices that support software updates, security updates and anti-virus products will be configured to perform such updates regularly or automatically.

Users must not circumvent or make any attempt to circumvent the administrative, physical and technical safeguards we implement and maintain to protect personal data and the school's ICT facilities.

7.3 Data protection

All personal data must be processed and stored in line with data protection regulations and the school's data protection policy.

This can be found on Google Drive ->Staff->Policies -> Current Policies ALL.

7.4 Encryption

The school ensures that its devices and systems have an appropriate level of encryption.

School staff may only use personal devices (including computers and USB drives) to access school data, work remotely, or take personal data (such as pupil information) out of school if they have been specifically authorised to do so by the headteacher.

Use of such personal devices will only be authorised if the devices have appropriate levels of security and encryption, as defined by the Assistant Head (Learning Technology)

8. Protection from cyber attacks

The school will:

- Work with governors and the IT department to make sure cyber security is given the time and resources it needs to make the school secure
- Provide annual training via GOSH GOLD for staff (and include this training in any induction for new starters on cyber security, information governance and counter fraud including how to:
    - Check the sender address in an email
    - Respond to a request for bank details, personal information or login details
    - Verify requests for payments or changes to information
- Make sure staff are aware of its procedures for reporting and responding to cyber security incidents
- Investigate whether our IT software needs updating or replacing to be more secure
- Not engage in ransom requests from ransomware attacks, as this would not guarantee recovery of data
- Back up critical data every evening and store these backups remotely on a NAS drive.
- Make sure staff:
    - Dial into our network using Cisco AnyConnect when working from home
    - Enable multi-factor authentication where they can, on things like school email accounts
- Have a firewall in place that is switched on
- Check that its supply chain is secure, for example by asking suppliers about how secure their business practices are and seeing if they have the Cyber Essentials certification

9. Internet access

The school wireless internet connection is secured and filtered by LGFL. If you encounter sites with inappropriate content that are not filtered, please report these to Assistant Head (Learning Technology) or Crossover Solutions who will add the website to the LGFL filter.

Staff must not give the WIFI password to anyone who is not authorised to have it. Doing so could result in disciplinary action. Parents and guests should use the NHS Public Wi-Fi.

10. Monitoring and review

The headteacher and Assistant Head (Learning technology) monitor the implementation of this policy, including ensuring it is updated to reflect the needs and circumstances of the school.

This policy will be reviewed every two years.

The governing board is responsible for approving this policy.

11. Related policies

This policy should be read alongside the school's policies found on **Google Drive ->Staff->Policies -> Current Policies ALL**:

- Staff handbook
- Online safety policy
- Safeguarding and Child Protection policy

- Data protection policy
- Behaviour Principles
- Staff laptop agreement
- Staff iPad agreement

12. Relevant legislation and guidance

This policy refers to, and complies with, the following legislation and guidance:

Data Protection Act 2018

The General Data Protection Regulation

Computer Misuse Act 1990

Human Rights Act 1998

The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000

Education Act 2011

Freedom of Information Act 2000

The Education and Inspections Act 2006

Keeping Children Safe in Education 2021

Searching, screening and confiscation: advice for schools

National Cyber Security Centre (NCSC)

Education and Training (Welfare of Children Act) 2021

13. Declaration (Acceptable Use Policy)

I have read the above and understand that if I infringe any of these rules I will lose access to and use of School facilities and further action (including disciplinary and/or criminal proceedings) may need to be taken.

Staff Name (Please print): ________________________________

Signed: ____

Date: ____

Appendix 1: Social Media guidance for staff

Don’t accept friend requests from pupils on social media

10 rules for school staff on Social Media

1. Change your display name – use your first and middle name, use a maiden name, or put your surname backwards instead
2. Change your profile picture to something unidentifiable, or if not, ensure that the image is professional
3. Check your privacy settings regularly
4. Be careful about tagging other staff members in images or posts
5. Don’t share anything publicly that you wouldn’t be just as happy showing your pupils.
6. Don’t use social media sites during school hours
7. Don’t make comments about your job, your colleagues, our school or your pupils online – once it’s out there, it’s out there
8. Don’t associate yourself with the school on your profile (e.g. by setting it as your workplace, or by ‘checking in’ at a school event)
9. Don’t link your work email address to your social media accounts. Anyone who has this address (or your personal email address/mobile number) is able to find you using this information
10. Consider uninstalling the Facebook app from your phone. The app recognises wifi connections and makes friend suggestions based on who else uses the same wifi connection (such as parents or pupils)

Check your privacy settings

Facebook

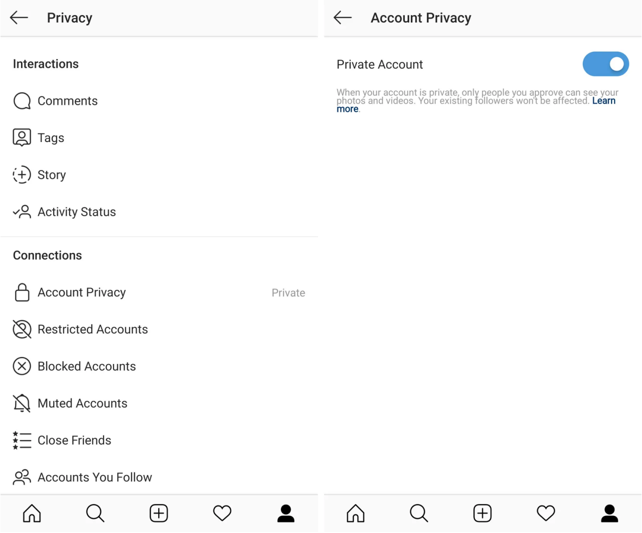
- Change the visibility of your posts and photos on Facebook to **‘Friends only’**, rather than ‘Friends of friends’. Otherwise, pupils and their families may still be able to read your posts, see things you’ve shared and look at your pictures if they’re friends with anybody on your contacts list
- Don’t forget to check your **old Facebook posts and photos** – go to bit.ly/2MdQXMN to find out how to limit the visibility of previous posts
- The public may still be able to see posts you’ve **‘liked’**, even if your profile settings are private, because this depends on the privacy settings of the original poster
- **Google your name** to see what information about you is visible to the public
- Prevent search engines from indexing your Facebook profile so that people can’t **search for you by name** – go to bit.ly/2zMdVht to find out how to do this
- Remember that **some information is always public**; your display name, profile picture, cover photo, user ID (in the URL for your profile), country, age range and gender

Instagram

Set your account to private. New people will now only see your name and profile image:

Go to Instagram's settings menu. It's hidden away on your profile page behind the hamburger button in the top-right corner. That will open a side menu with several choices; you can access your settings from the cog that appears at the very bottom.

From there, go to "Privacy" > "Account Privacy" and activate the "Private Account" setting.



Account Privacy: Private

Private Account ●

When your account is private, only people you approve can see your photos and videos. Your existing followers won't be affected. Learn more.

Remember that, even with private accounts, your followers can still take a screenshot of any of your posts and still share your content.

Twitter (X)

- If you have a Twitter (X) account specifically for or about teaching, make sure you don't include identifying information about yourself or your school. Use a nickname, for example 'Miss M'
- Change the visibility on your birth date to 'You follow each other' to prevent pupils and parents seeing this personal information. See Twitter's profile visibility guidance for more support
- Remember, your username, biography, location, website and profile picture are always public and can be seen by pupils and parents, even if they don't follow you and you have protected your tweets
- Protect your tweets by checking the box in the 'Audience and tagging' section of your privacy settings. This will mean only your approved followers can see your tweets Google your name to see what information about you is visible to the public

What to do if...

A pupil adds you on social media

- In the first instance, ignore and delete the request. Block the pupil from viewing your profile
- Check your privacy settings again, and consider changing your display name or profile picture
- If the pupil asks you about the friend request in person, tell them that you're not allowed to accept friend requests from pupils and that if they persist, you'll have to notify senior leadership and/or their parents. If the pupil persists, take a screenshot of their request and any accompanying messages
- Notify the senior leadership team or the headteacher about what's happening

A parent adds you on social media

- It is at your discretion whether to respond. Bear in mind that:
    - Responding to one parent's friend request or message might set an unwelcome precedent for both you and other teachers at the school
    - Pupils may then have indirect access through their parent's account to anything you post, share, comment on or are tagged in
- If you wish to decline the offer or ignore the message, consider drafting a stock response to let the parent know that you're doing so

You're being harassed on social media, or somebody is spreading something offensive about you

- **Do not** retaliate or respond in any way
- Save evidence of any abuse by taking screenshots and recording the time and date it occurred
- Report the material to Facebook or the relevant social network and ask them to remove it
- If the perpetrator is a current pupil or staff member, our mediation and disciplinary procedures are usually sufficient to deal with online incidents
- If the perpetrator is a parent or other external adult, a senior member of staff should invite them to a meeting to address any reasonable concerns or complaints and/or request they remove the offending comments or material
- If the comments are racist, sexist, of a sexual nature or constitute a hate crime, you or a senior leader should consider contacting the police