Guildhouse School
43-45 Bloomsbury Square, London, WC1A 2RA
Tel: +44 20 7841 1580
www.guildhouseschool.com

ICT Acceptable Use Policy

Date of policy review:	September 2023
Date for review:	September 2024
Lead for review:	Assistant Headteacher (AHPP)

GUILDHOUSE SCHOOL
LONDON

Guildhouse School
43-45 Bloomsbury Square, London, WC1A 2RA
Tel: +44 20 7841 1580
www.guildhouseschool.com

Contents

Guildhouse School
43-45 Bloomsbury Square, London, WC1A 2RA
Tel: +44 20 7841 1580
www.guildhouseschool.com

Purpose

The purpose of this policy is to ensure that all students studying at Guildhouse School London are fully conversant on the acceptable use of Information and Communication Technology (ICT) resources provided by CATS Global Schools (CGS) for all students. Our goal is to promote educational excellence by facilitating resource sharing, innovation, and communication in a safe and secure environment. This also includes ensuring that personal, sensitive and/or confidential information is protected from unauthorised access and is accessible only to those with a legitimate right to access to which intellectual property applies. As part of the Induction process to the school, students are required to read through and agree to the ICT Acceptable Use Agreement and have the opportunity to clarify anything.

Scope

This policy applies to all students who access and use the ICT resources provided by CGS, whether on-premises or remotely.

General Security

The following security controls must be applied by students to safeguard IT Services and information assets.

- Always lock your screen when away from your desk
    - For Windows devices use CTRL-Alt-Del and Lock this Computer or Windows button + L
    - For Mac devices use CTRL-Shift-Eject, or CTRL-Shift-Fn-Power
- Never leave portable equipment unattended, lock it away when not in use
- Never load unauthorised software to school computers without first checking with IT
- Any breaches or risks relating to the security of information and IT assets must be reported to school staff.

IT systems will be monitored using audit trails and log files to ensure appropriate use, any misuse will be subject to investigation and may lead to disciplinary action in line with the school disciplinary ladder, or criminal proceedings.

GUILDHOUSE SCHOOL
LONDON

Guildhouse School
43-45 Bloomsbury Square, London, WC1A 2RA
Tel: +44 20 7841 1580
www.guildhouseschool.com

Username and Passwords

Individual Accounts

Students are personally responsible for the security of their individual login details and will be held responsible for any activity carried out using their login details. Passwords, PINs and access codes must not be shared with anyone. Passwords must not be written down and left visible to others, or kept with mobile devices e.g., Laptops, iPads. Passwords must be hard to guess and contain at least twelve characters, The minimum password requirement is that it must include three of the four following types of character:

- **Number**
- **Lower case letter**
- **Upper case letter**
- **Special character such as: ! # £ $**

Passwords should be changed at regular intervals; the system is configured to automatically force password changes and to prevent reuse of passwords. Users are held accountable for all activity undertaken using their account. If you suspect that someone else may know your password, you must change it immediately using the change password function, if available, or by contacting the IT Service Desk or appropriate system administrator.

If you anticipate that someone else needs access to data held within your account, you must arrange for data to be transferred in advance.

Confidentiality

Confidentiality ensures that sensitive information is accessible only to those authorised to have access. At CGS, we prioritise the protection of all confidential information, including but not limited to, personal data, academic records, communication, and proprietary information.

Student Responsibilities
Every student is entrusted with the responsibility of maintaining confidentiality. As such:

- Students must not disclose, disseminate, or use confidential information without appropriate authorisation.
- When working on assignments, projects, or other academic work that involves sensitive or personal information, students must take care to prevent unauthorised access or disclosure.

Guildhouse School
43-45 Bloomsbury Square, London, WC1A 2RA
Tel: +44 20 7841 1580
www.guildhouseschool.com

- Confidential information should never be stored on personal devices or transmitted over unsecured networks.
- Any accidental disclosure or loss of confidential information must be reported to school authorities or the IT Service Desk immediately.
- Students are required to log out or lock devices when not in use, especially in shared or public spaces.
- Under no circumstances should any information of a confidential or sensitive nature be placed on the internet.

Data Protection and Privacy

- CGS complies with all applicable data protection laws and regulations.
- Personal data of students will not be shared, sold, or disclosed to third parties without consent, except where required by law or for legitimate educational or administrative purposes.
- All stored personal data is kept secure with appropriate security measures in place to prevent unauthorised access, alteration, disclosure, or destruction.

Digital Communication

- Email and other forms of digital communication provided by CGS are to be used responsibly. Sharing of confidential information should be done judiciously and, where possible, with encryption.
- Students should be wary of phishing attempts and not respond to unsolicited requests for personal or sensitive information.

Consequences of Breach

- Breaching confidentiality, whether intentionally or due to negligence, may result in disciplinary action. This can range from warnings and mandatory training to more severe consequences as outlined in the Student Handbook, including potential legal ramifications.

Copyright and Intellectual Copyrights

Most information and software is subject to copyright or other intellectual property rights protection. CGS systems must not be used to store, send, receive, or view any material that there is reason to suspect may be in breach of copyright. There are serious implications for both CGS and the individual if an organisation is found to be in breach of legislation relating to copyright.

Software

Only licensed and approved software may be used on CGS systems. The use of or copying of software is subject to licensing and copyright restrictions and is not permitted unless it is within the remit of the licence agreement. There are serious implications for both CGS and individuals if an organisation is found to be using illegal copies of software or are inadequately licensed. The copying of software for personal use is not permitted. CGS will treat any unauthorised use or copying of software as a serious breach of policy.

Guildhouse School
43-45 Bloomsbury Square, London, WC1A 2RA
Tel: +44 20 7841 1580
www.guildhouseschool.com

Software downloaded from the Internet must not be installed on CGS systems without written authorisation from the ICT department.

Malware, Viruses and SPAM

All IT equipment that has connectivity to CGS network MUST have up to date virus protection software installed and must be updated with relevant software patches. CDs or removable media from untrusted sources may contain viruses and should not be used on CGS systems. E-mails may contain viruses or malicious code that can cause disruption to IT systems.

Any e-mails and attachments that have been received from unknown or untrusted sources should not be opened but should be reported to the IT Service Desk, as should excessive quantities of unsolicited e-mail and junk mail / SPAM. Knowingly distributing a virus or malicious code or failing to act responsibly to protect CGS systems from disruption will be considered a breach of this policy.

Web Filtering

Filtering and monitoring are both important parts of safeguarding students from potentially harmful and inappropriate online material.

To ensure a safe online environment, CGS employs web filtering solutions to restrict access to inappropriate, illegal, or harmful web content. This is controlled by the IT Infrastructure team within CGS. On a monthly basis, comprehensive Web Usage reports are prepared which are distributed to the Designated Safeguarding Lead (DSL) at Guildhouse School. These reports provide critical insights into various metrics including Overall Web Activity, Most Visited Categories, Most Visited Sites, Web Browsing Time, attempts to access blocked sites, Proxy Avoidance and other essential data by username. How to interpret these reports has been explained to the DSL by the Designated Governor for Safeguarding. It is worth noting that out current web filtering service provider is an accredited member of the Internet Watch Foundation (IWF), Counter-Terrorism Internet Referral Unit list (CTIRU), and blocks access to illegal content including child sexual abuse material (CSAM). The Filtering software also blocks newly created web sites until they become categorised by the Web filtering Service Provider.

Clear roles, responsibilities and strategies are vital for delivering and maintaining effective filtering and monitoring systems. It's important that the right people are working together and using their professional expertise to make informed decisions.

To understand and evaluate the changing needs and potential risks the Designated Governor for Safeguarding, DSL, and the IT team review the effectiveness of the provision and the filtering and monitoring system itself annually, documenting decisions on what is blocked or allowed and why. There is also the opportunity for what is blocked or allowed to be altered during the year if trends are identified by the DSL or there is a change in working practice or the introduction of new technology.

The appropriately qualified CGS IT Team has the technical responsibility for:

- maintaining filtering and monitoring systems
- providing filtering and monitoring reports
- completing actions following concerns or checks to systems

Guildhouse School
43-45 Bloomsbury Square, London, WC1A 2RA
Tel: +44 20 7841 1580
www.guildhouseschool.com

The CGS IT Team works with the Senior Leadership Team, governors and DSL to:

- procure systems
- identify risk
- carry out reviews
- carry out checks

Attempting to bypass or disable the web filters, or accessing proxy sites to circumvent the filter, is strictly prohibited and may result in disciplinary action.

Students who believe a website is being blocked in error or feel that a website should be blocked may submit a request for review to a teacher or the IT Service Desk.

Application Filtering

CGS restrict access to specific applications to ensure network security, manage bandwidth, and maintain an academic focus. Installation of unauthorised software or apps on CGS devices is prohibited. Any attempt to bypass application filters will be deemed a violation of this policy.

Captive Portal Usage

Before accessing the Internet, students are prompted to authenticate through a captive portal, providing their assigned username and password.
The captive portal serves as a checkpoint to verify the user's identity and ensure the security of our network resources. Sharing credentials or attempting to impersonate another student/user is strictly prohibited. Any unauthorised attempt to bypass the captive portal will result in disciplinary action.

Social Networking

Social Networking platforms, such as Facebook, Twitter, Instagram, and LinkedIn, are tools that facilitate connections, sharing of information, and community-building. While they offer numerous benefits, their use within an educational context must be balanced with appropriate conduct to ensure the safety, respect, and privacy of all members of the CGS community.

Approved Use

- Official CGS accounts on social networking platforms will be managed by designated staff. These accounts represent the institution and must adhere to its ethos, branding, and communication guidelines.
- When representing CGS on social media, either through an official account or personal profile, it is ensured that content aligns with the institution's values and standards.

Student Responsibilities

- When using personal social media accounts, students should differentiate personal opinions from those of CGS.

Guildhouse School
43-45 Bloomsbury Square, London, WC1A 2RA
Tel: +44 20 7841 1580
www.guildhouseschool.com

- Harassment, hate speech, or any form of discrimination is strictly prohibited, even on personal accounts.
- Always maintain a level of professionalism and respect. Avoid posting content that could harm your reputation or that of CGS.
- Respect copyright laws: do not post copyrighted material without appropriate permissions.
- Be cautious of friend or connection requests from unknown individuals and avoid sharing sensitive personal information on these platforms.

Best Practices

- Engage positively and constructively. Use social networking platforms to enhance learning, share achievements, and build community.
- Think before posting. Remember that content on the internet has a long lifespan and wide reach.
- Regularly review and adjust privacy settings on your accounts to match your comfort level and security needs.

Consequences of Misuse

- Misuse of social networking platforms, including breaches of privacy, sharing inappropriate content, or any behaviour that harms the reputation of CGS, may lead to disciplinary action, up to and including suspension and/or permanent exclusion. Or legal proceedings.

Use of Personal Equipment by Students

Students may use their own digital equipment to enhance their education experience and facilitate communications with their parents or guardians, however students must adhere to the following policiesand responsibilities. Any use of personal equipment is at the discretion of the school.

- Student equipment may not be directly connected to a wired network point in student houses & accommodation. Students are not permitted to connect personal equipment to any wired networks within the schools, classroom, cafeteria, or any other school location.
- Students may connect to clearly designated school Guest or Student wireless networks only.
- Students are expected to maintain appropriate, up to date, Antivirus, Anti-Spam and Anti Malware software on any machine they connect to school networks.

Building Student Resilience through Education

Students at Guildhouse School London are taught about online safety and harms as part of the PSHE/RSE curriculum. This includes being taught about:

- what positive, healthy and respectful online relationships look like
- the effects of their online actions on others
- how to recognise and display respectful behaviour online

Guildhouse School
43-45 Bloomsbury Square, London, WC1A 2RA
Tel: +44 20 7841 1580
www.guildhouseschool.com

In these sessions, teachers also address online safety and appropriate behaviour in an age-appropriate way that is relevant to equip students with the knowledge needed to make the best use of the internet and technology in a safe and respectful way.

Parental Engagement regarding Online Safety

Guildhouse School London informs, communicates and educates parents/carers in online safety by including a reference of Online Safety advice (NSPCC) as part of the start of term school parental engagement regarding RSE so as to work together with the school to keep students safe online (please see appendix).

CATS College London Limited trading as Guildhouse School - Registered in England: 07442735
Registered Office: Suites 6-7 The Turvill Building Old Swiss, 149 Cherry Hinton Road, Cambridge, England, CB1 7BX

GUILDHOUSE SCHOOL
LONDON

Guildhouse School
43-45 Bloomsbury Square, London, WC1A 2RA
Tel: +44 20 7841 1580
www.guildhouseschool.com

Appendices

Appendix 1: Parental Engagement regarding Online Safety Advice (as part of Autumn Term HT1 Reporting

Online safety: top tips

Going online is a huge part of most young people's lives so it's important to talk to them about online safety. Here's our tips to get you started.

Chat to them about what they like to do online

The best way to find out what your child is doing online is to talk to them and have regular conversations so that online safety is part of everyday discussion. Ask them open-ended questions like 'What's your favourite game or app to play on?'.

- Listen to what they have to say and show an interest. They could give you a demo of their favourite app or show you their favourite YouTube or TikTok account.
- They will probably be able to teach you things you don't know! This will also give you an opportunity to chat about any safety settings they might already have in place.
- Regular conversations with your child will encourage them to come to you if they ever need support or advice.

Talk about who they are in contact with online

There are lots of different ways that children can talk to people online – messaging apps, on social media, and less obvious ways such as chat on online games. Talk to your child about who they are talking to and what they are sharing with them.

- Use settings to help limit who can contact your child.
- Remind your child that they shouldn't share personal information with people they don't know online.
- Let your child know they can come to you or another trusted adult if any conversation makes them feel uncomfortable.

- App or game settings – in-app tools that can help to keep your child's account private and manage who they're talking to. You can normally find information on these in account settings or directly on the platforms website.
- Mobile or network provider settings – help to manage browsing access and stop your child from visiting inappropriate sites or downloading apps that aren't suitable. Contact your mobile or broadband provider for more information about setting this up.

Remember it's ok to ask for help!

Remember you don't have to be an online safety expert – that's our job! We're here to help, with resources and advice to help support you and your child.

If your child asks you a question you don't know the answer to, or speaks to you about a negative experience they had online, here are some of things you could do:

- Visit the NSPCC online safety hub: **nspcc.org.uk/onlinesafety**
- Call the NSPCC helpline **0808 800 5000** to speak to an advisor
- Ask another parent
- Speak to your child's teacher
- If your child needs more support, they can contact Childline: **childline.org.uk**

NSPCC

EVERY CHILDHOOD IS WORTH FIGHTING FOR

GUILDHOUSE SCHOOL
LONDON

Guildhouse School
43-45 Bloomsbury Square, London, WC1A 2RA
Tel: +44 20 7841 1580
www.guildhouseschool.com

Additional Useful Links

Keeping children safe online | NSPCC

How to Ensure Your Children Stay Safe While Playing Online Games | NSPCC

Social media | NSPCC

Internet connected devices | NSPCC

Online wellbeing | NSPCC

Use Parental Controls to Keep Your Child Safe | NSPCC