ICT Policy - STUDENT

Effective date: June 2024

Job role of author: Director of Facilities & Technical Services

Review date: June 2025

Approved by: P&PG

Introduction

All Staff and students share the ICT facilities at Hugh Baird College. These facilities must be used responsibly by everyone on and off-site, since misuse by even a few individuals has the potential to negatively impact productivity, disrupt College business and interfere with the work or rights of others. Therefore, all staff and students are expected to exercise responsible and ethical behaviour when using the College's Information Communication Technology facilities. Any action that may expose the College to risks of unauthorised access to data, disclosure of information, legal liability, or potential system failure is prohibited and may result in disciplinary action up to and including cessation of study programme.

This policy covers the following key aspects:

- College network
- Electronic Mail
- Social Media
- E-Safety

This policy applies to all students at Hugh Baird College and include on-site and off-site access. There are further policies that relate to students. It is the responsibility of Progress Coaches to ensure that all ICT policies are clearly communicated, understood and followed.

Additionally, students may also be required to adhere to 3rd party policies / guidelines, such as those issued by partner Higher Education Institutions. Specific guidance will be provided within course/ module handbooks.

Failure to adhere to this policy may result in disciplinary action.

Usage of the College Network

The College network is defined as all personal computers (including laptops and tablets), printers and devices connected to the physical and wireless network and associated services, i.e. the Internet. This includes devices not owned by the College, i.e. student devices connected to the College's "Guest" wireless network.

All users using devices falling within this definition must adhere to the following guidelines:

General

- Users are responsible for the use, activity and compliance of their network account and associated services, i.e. Internet activity;
- Any attempt to move, harm or destroy any computer / network hardware or the data of another user will be considered as vandalism and is strictly prohibited;
- Users must not attach unauthorised hardware devices not approved by the College to the College network;
- Games are not permitted unless authorised by the ICT Services Manager (ISM);
- The time period between 12:30 AM and 5:00 AM is considered a maintenance period and access to systems / services may be disrupted without prior notification. Users will be given prior notification of any maintenance taking place outside of these times;

Data security / allocation / retention

- Use of the network for any illegal activities, such as hacking, is strictly prohibited. It is gross misconduct, and a criminal offence under the terms of the Data Protection Act 2018 / GDPR 2018, to disclose personal data to any person not authorised to receive it.
- Users will be allocated a proportion of the storage space on the network appropriate to their course and the availability of storage. Additional space may be made available at the discretion of the ICT Services Manager and users may only use the network space allocated to them;
- No guarantee can be made by the College regarding the privacy or security of data held within individual user network accounts. This also applies to other associated services, i.e. email;
- Members of the ICT Services team have access to all accounts and messages, any inappropriate files, data or messages may result in the

suspension of the network account and could lead to disciplinary action including dismissal;

- Users must not deliberately introduce any virus, worm, Trojan horse or any other "nuisance" program or file onto any system or take deliberate action to circumvent any precautions taken by the College to prevent "infection" of its machines;
- Users wishing to access USB storage devices using staff computers will be required to password protect and encrypt their USB devices prior to use;
- Users should not store sensitive data on local workstations or on portable devices such as USB pen drives. In line with the College's Data Protection Policy users are reminded to consider whether the storage of sensitive data is appropriate;
- The storage of copyrighted material, such as music and video files, is prohibited;
- Data stored on network shares will be backed up on a daily basis;
- Deleted files will be kept on the backup system for a maximum of 60 days;
- Access to third party remote desktop tools is prohibited;
- Monthly archives will be kept for 365 days;
- The College electronic mail solution is facilitated by the Microsoft 365 service. As such users are subject to the backup, storage and retention limitations as defined by the relevant subscription.
- Any activity that is likely to damage the reputation of the JANET network will also be regarded as unacceptable use of the College Network.

Your account

- users must set their password so that it contains a minimum of 12 characters, you will be prompted to change your password when you first access your account;
- You will be given a grace period of 30 days from the start of term to register to use multi-factor authentication (MFA). If you do not register for MFA, you will not be able to access your account when away from the College. Details of the MFA facility can be found on the student section o the College website;
- user accounts not used for 100 days will be automatically removed;
- password changes can only be requested in person by the account owner upon production of a valid student ID card or by using the Self Service

Password Reset facility. Details of the Self-Service Password Reset facility can be found on the student section of the College website;

- Users will not be required to periodically change their passwords, but in the event of suspicious activity the ICT Services team may force a password change.

Internet Access

The College has implemented content filters to protect users from unsavoury and illegal Internet sites.

Requests for access to the specific sites contained within these categories, for curriculum purposes, should be made via your tutor. The viewing of Internet sites containing pornography, racist or other inappropriate material is specifically banned when using College equipment.

The College leverages the browser safe search feature to protect users. As a result content may be prohibited by ancillary solutions outside of the administrative control of the ICT Services team.

The ICT Services team record all Internet usage.

Monitoring

The monitoring of student network activity, i.e. Internet history, file stores and PC activity, will be routinely undertaken.

Usage of Electronic Mail

The College Electronic Mail system is defined as the hardware, software and services the College provides to access and facilitate accounts with an address ending in "hughbaird.ac.uk", "seftonsixth.ac.uk" or "sssfc.ac.uk". This includes access to College electronic mail from outside the College, i.e. staff or students accessing electronic mail from home.

Usage of electronic mail falling within this definition must adhere to the following guidelines:

General

- All e-mail and associated system resources are the property of Hugh Baird College;
- Users are responsible for the usage, activity and compliance of their electronic mail account;
- Access to the "All Staff" and "All Student" distribution lists is restricted.

Users may not:

- Use the College electronic mail system to pursue the interest of other organisations beside Hugh Baird College;
- Use email for commercial solicitation;
- Use email for the interests of groups of staff or students except for Hugh Baird College business;
- Use email to distribute hoaxes, chain letters, or advertisements; and/or send rude, obscene, racist or harassing messages or pictures; or propagate viruses, knowingly or maliciously. This list is not exhaustive, nor exclusive;
- Users must not send, forward and/or reply to large distribution lists concerning College business;
- The subject line and body text of emails that originate from outside of the College will be amended to include the subject line and body warning text;

Data security / allocation / retention

- Users are responsible for sharing their own mailbox features, i.e. Calendars and Inbox. The ICT Services team will not amend mailbox permissions unless specifically authorised to do so by the ICT Services Manager for purposes of support;
- Electronic mail is a record and therefore the management of electronic mail and the users of email must comply with all applicable legislation, regulations, policies and standards (e.g. the Data Protection Act). This includes complying with copyright and licence provisions with respect to both programs and data;
- The College electronic mail solution is facilitated by the Microsoft 365 service. As such users are subject to the backup, storage and retention limitations as defined by the relevant subscription.

Monitoring

- By default ICT Services staff will not be granted administrative access to student mailboxes. Access will be granted to complete specific work and revoked once completed, the ISM will review audit logs to identify potential breaches of this policy;
- The monitoring of student mailboxes will be routinely undertaken.

Social Media

Social media is a useful tool and Hugh Baird College understand that students communicate via services such as Instagram and Snapchat. However, there are also risks attached to the use of social media and students are expected to use it responsibly whilst connected to the College network whether this be on a College device or a personal device.

All users must adhere to the following guidelines when accessing social media sites through the College network or on College premises.

- Use of sexually explicit language or viewing, creation or sharing of sexually explicit imagery is not permitted nor advised from a safeguarding perspective;
- Verbally abusive or threatening language is not tolerated;
- Use of racist or extremist language which would directly contravene British and College values, as detailed in the Prevent strategy, is not permitted;
- Use of social media for the purposes of radicalisation or the expression of extremist views is not permitted;
- Communication with staff members unless on a College established social media site is not permitted. Any such communication instigated by staff members to a student's personal social media should be reported to safeguarding team.

Please be mindful of the following when using social media.

- Don't post anything on social media that you wouldn't want others to see. Remember what you post could impact on your future career;
- Don't be pressured into doing anything inappropriate on social media like posting photos or videos;
- Don't accept people as friends or engage in conversations on social media if you don't know the people you are communicating with, be aware of "stranger danger".

General guidelines

- Exercise caution when accessing personal social media sites in a public environment, e.g. a classroom or library;
- If your social media profile lists that you are a student at the College, it should also state that any views expressed are your own and do not represent the College;
- Set any profiles to “private” to ensure control over who is able to access / view your information. Recommended privacy settings are available from the ICT Helpdesk;
- Ensure conduct on sites could not be seen as detrimental to the College or bring the College into disrepute;
- Be security conscious and take steps to protect yourself from identity theft, for example by restricting the amount of personal information given out. Social media websites allow people to post detailed personal information such as date of birth, place of birth and favourite football team, which can form the basis of security questions and passwords;
- Where possible also employ the services of the multiple factor authentication features (MFA) offered the platform;
- Change your social media password often. The ICT Helpdesk can provide advice concerning password security if required.

General Guidelines

General

- Report any incidents of vandalism, abuse or malfunction to your tutor immediately;

Good practice

- Users are encouraged to change their passwords on a regular basis to maintain the security of their accounts;
- Do not reveal your network password to anyone. Remember, you are responsible for the activity of any accounts or devices associated to you;
- Do not leave any devices unattended whilst logged in.

Laptop Usage

- Before using your laptop ensure that you adopt a posture in which you can keep your wrists straight, your shoulders relaxed and your back supported, and in which you feel comfortable;
- While using your laptop place it on a desk or table, do not support the laptop on your lap because of the potential hazards of heat transfer;
- Take a short break at least once an hour;
- Rest your eyes frequently by looking at something far away or by closing them;
- Adjust the screen angle and height to reduce stretching your neck and to minimize the glare on the screen;
- If possible attach a full size keyboard and mouse to your laptop;
- If you're connecting your laptop to the mains ensure that the cables do not present a trip hazard;
- If using your laptop connected to a wireless network ensure that the laptop base is at least 15cm from your body.

Keeping yourself safe online

Hugh Baird Colleges encourages all students to make good use of online resources including social media. The Internet can be a rich source of information and a great way to network, however it is important that this is done safely. Below is some guidance about how to work online safely.

- It is a warning sign if someone only wants to talk to you in secret and they are asking you not to tell anyone about your conversations;
- Never agree to talk to anyone in secret, especially if they are threatening you not to tell anyone about it. Always inform a trusted adult of your online conversations;
- It isn't OK for someone online, who you don't know, to insist on taking your phone number or address;
- Never give out personal details such as your name, address or phone number and never tell anyone which school/college you go to. Keep your personal details private. In the wrong hands, these details can be used to find you, meaning you may become at risk;
- If you are sent an email that makes you feel uncomfortable or worried speak to an adult or visit the POD. For example, the person emailing you may say things or send you embarrassing/inappropriate pictures. In addition, the person could be insisting that you use a webcam or send them photographs of yourself that make you feel uncomfortable. **This is never OK** and you should never send anyone, including those you meet online, photo of yourself that may make you feel uncomfortable;
- Always tell a trusted adult if someone makes inappropriate comments or suggestions or makes you feel uncomfortable;
- Never agree to meet anyone you have met online on your own. Only meet someone you have met online in a public place with one of your parents or another trusted adult.

The risk of radicalisation online

Extremist groups are known to use the internet and social media to communicate with vulnerable young people and spread radical messages, aiming to gain more recruits and supporters. When the internet is used safely and responsibly, there are lots of positive opportunities for people to learn so it's important to be aware of negative influences online.

Try to remember the following, it will help you to keep safe from extremism and radicalisation online:

- Don't view people you have encountered on social media or through online games as 'online friends'. They are strangers, it's important to remember that it's easy for people to lie about themselves online;
- Extremism comes in many forms, it doesn't have to be in relation to skin colour, race or religion. If someone is expressing their views in an aggressive or inappropriate manner you should disengage with this conversation and block them or report them to the Safeguarding team or the POD;
- Do not follow or like extremist groups on social media, this provides them with opportunities to contact you to express extreme views;
- Do not force your opinions or views on others online, this can be classed as extremist and may make others feel uncomfortable;
- Hate language such as homophobic, transphobic or racist insults is inappropriate and extreme. You do not have to accept it and you should report this to the Safeguarding team or the POD.

If you are concerned about anything you encounter online, you can seek help and support from staff in POD or you can refer to the Safeguarding team by using the referral button on Student Zone or the College website.

There are also some useful websites to help you learn more about online safety. If you are concerned about something, you can call the NSPCC's online safety helpline on 0808 800 5002.

Additional resources can be found here:

- http://educateagainsthate.com/parents/online-radicalisation
- https://www.childnet.com/resources/supporting-young-people-online

Must do / must not do

What you **must do**

- **You must** report any requests you may receive through social media to post sexually explicit or offensive imagery online;
- **You must** report to a safeguarding officer if you view any extremist or radical views expressed online;
- **You must** report any personal communication staff may make with you via social media;
- **You must** immediately tell a Safeguarding Officer if you receive offensive or inappropriate messages whilst at the College. This includes messages sent to your personal mobile phone or via Microsoft Teams;
- **You must** immediately tell a lecturer or your personal tutor if you think your network account has been tampered with;
- **You must** ensure all emails sent using your College email address to external organisations are carefully written and authorised by your tutor before sending;
- **You must** follow the rules of the ICT Policy;
- **You must** ensure that any content posted is appropriate and abides by existing College policies when using Wiki or Blog sites;
- **You must** ensure links to external sites are appropriate when using College Wiki or Blog facilities;
- **You must** ensure copyrighted materials, such as pictures, are only added with the owner's permission when using College Wiki or Blog facilities.

What you **must not do**

- **You must not** upload explicit or offensive imagery to social media sites;
- **You must not** use College network to express extremist or radical views;
- **You must not** communicate with staff via personal social media accounts, unless through a College established social media site such as a course specific Facebook site;
- **You must not** take or upload images of any staff or students;
- **You must not** discuss issues relating to staff or students at Hugh Baird which may bring the College into disrepute;
- **You must not** make or receive mobile telephones calls or text message during lessons;
- **You must not** reveal personal details of yourself or others in e-mail communication, or arrange to meet anyone you have met electronically;
- **You must not** forward chain letters;

- **You must not** send abusive or inappropriate emails, text messages or in any other way participate in the misuse of technology;
- **You must not** publish personal details on public websites, i.e. Wiki's and Blogs;
- **You must not** publish comments that may be seen as offensive when using websites.

Responsibilities

User

- Users are responsible for ensuring that their use of the outlined systems is appropriate and consistent with this policy. Users must comply with any additional instructions or regulations displayed alongside computing facilities.

Departmental / specific

- The Director of Facilities & Technical Services is responsible for the implementation and compliance of the policy;
- The Student Services Manager is responsible for logging all e-Safety / Safeguarding issues;
- The ISM is responsible for ensuring all Internet activity is logged;
- There is a dedicated safeguarding team on site to support all students to stay safe. They can all be contacted by accessing the POD on a drop in basis.

Name	Location
Alex Lang	5th Floor
Sonia Stirling	5th Floor
Tony Cooke	5th Floor
Owen Rogers	POD, ground Floor, Balliol
Michelle Ferguson	POD, ground Floor, Balliol
Julie Brennan	POD, ground Floor, Balliol
Linda Marsh	POD, ground Floor, Balliol
Janine Hopewell	POD, ground Floor, Balliol
Pam Cotter	1st Floor Learner Support Office
Matt Wilson	1st Floor Learner Support Office
Jenny Quinn	POD, ground Floor, Balliol
Julie Bass	South Sefton POD
Liam Mathews	South Sefton POD
Christina McCoy	South Sefton POD

If you would prefer to make an anonymous referral then the safeguarding form can be completed via student zone by pressing the "Safeguarding" icon.

Inclusion statement

Hugh Baird College is proud to promote an inclusive environment for all students regardless of age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex and sexual orientation in accordance with the Equality Act 2010. As a college it is recognised that diversity of all forms should be celebrated. This is promoted to ensure all staff, students and stakeholders feel proud to explore and share their own identity.

Hugh Baird College

Balliol Road
Bootle
Liverpool
L20 7EW

Telephone
0151 353 4444

Email
enquiries@hughbaird.ac.uk

www.hughbaird.ac.uk