ICT ACCEPTABLE USE POLICY

HARTPURY

INTRODUCTION
It is the responsibility of all users of the Hartpury network to read, understand, accept and abide by this policy. This policy may be updated from time to time, in order to comply with legal and Information Security Policy requirements.

1.1 Purpose
This Acceptable Use Policy is intended to provide a framework for such use of Hartpury's IT resources. It should be interpreted such that it has the widest application and to include new and developing technologies and uses, which may not be explicitly referred to.

1.2 Policy
This Acceptable Use Policy is taken to include the JANET Acceptable Use Policy (section 8) and the JANET Security Policy published by JANET (UK), the Combined Higher Education Software Team (CHEST) user Obligations, together with its associated Copyright Acknowledgement, and the EdUserv General Terms of Service. Hartpury also has a statutory duty, under Section 26 of the Counter Terrorism and Security Act 2015, termed "PREVENT". The purpose of this duty is to aid the process of preventing people being drawn into terrorism and/or extremism. A link to the JANET Acceptable use policy can be found in the section 8.

1.3 Scope
Users of Hartpury's facilities are bound by the provisions of its policies in addition to this Acceptable Use Policy. Hartpury seeks to promote and facilitate the positive and extensive use of Information Technology in the interests of supporting the delivery of learning, teaching, innovation and research to the highest possible standards. This also requires appropriate and legal use of the technologies and facilities made available to users.

2. UNACCEPTABLE USE

a) Subject to exemptions defined in 2f), the network or equipment, whether on site or remotely, may not be used directly or indirectly by a user for the download, creation, manipulation, transmission or storage of:

1. any offensive, obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material;
2. unlawful material, or material that is defamatory, threatening or discriminatory
3. Any material that promotes extremism or has the potential to radicalise themselves or others;
4. unsolicited "nuisance" emails to themselves or others;
5. material which is subsequently used to facilitate harassment, bullying and/or victimisation of a member of Hartpury or a third party;
6. material which promotes discrimination on the basis of race, gender, religion and belief, disability, age, sexual orientation, gender reassignment, pregnancy and maternity or marriage and civil partnership;
7. material with the intent to defraud or which is likely to deceive a third party;
8. material which advocates or promotes any unlawful act;
9. material that infringes the intellectual property rights or privacy rights of a third party, or that is in breach of a legal duty owed to another party; or
10. material that brings Hartpury into disrepute.

b) The network or equipment must not be deliberately used by a user for activities having, or likely to have, any of the following characteristics:

1. intentionally wasting staff effort or other Hartpury resources;
2. corrupting, altering or destroying another users' data without their consent;
3. disrupting the work of other users or the correct functioning of the network; or
4. denying access to the network and its services to other users.
5. pursuance of non-Hartpury approved commercial activities (even if in support of University/College business), subject to a range of exceptions.

c) Any breach of industry good practice that is likely to damage the reputation of the JANET network will also be regarded prima facie as unacceptable use of the network.

d) Where the Hartpury network or its equipment is being used to access another 3rd party network, any abuse of the acceptable use policy of that network will be regarded as unacceptable use of the Hartpury network.

e) Users must not:

- introduce data-interception, password-detecting or similar software or devices to the Hartpury network;
- seek to gain unauthorised access to restricted areas of Hartpury's network;
- seek to bypass security or safeguarding measures such as URL or application filters;
- access or try to access data where the User knows or ought to know that they should have no access;
- carry out any hacking or malicious activities;
- intentionally or recklessly introduce any form of ransomware, spyware, computer virus or other potentially malicious software;
- use cloud storage other than Microsoft OneDrive or Microsoft Teams for Hartpury business unless there is a proven reason to do so;
- use Hartpury network or equipment for crypto currency mining.
- Staff shall not use removable media unless there is a business case to do so and the media is encrypted.

f) Exemptions from Unacceptable Use: There are a number of legitimate academic activities that may be carried out using Hartpury's network that could be considered unacceptable use, for example, research involving defamatory, discriminatory, or threatening material, the use of images which may depict violence, the study of hate crime, terrorism related material or research into computer intrusion techniques. In such circumstances advice should be sought if potentially illegal material is involved and/or notification made to the Hartpury's Designated Safeguarding Lead (or Deputy) or Hartpury's Prevent Lead if the material relates to the promotion of extremism/terrorism prior to the introduction of said material onto the Hartpury network.

g) When using Hartpury computing facilities users MUST:

- log out of your account if you are leaving a computer unattended for an extended period of time, or otherwise lock the screen if you leave the keyboard and computer.

- take appropriate actions to physically secure equipment issued to you for the purposes of study or work.
- Install updates as soon as possible when instructed to do so.
    - Some updates may require returning to IT to be completed. If these are critical or security patches, they must be completed within 14 days.
- Use a unique login name. Generic and shared usernames are not permitted.
- Use a Password that follows the Password Policy.
- Use MFA (Multi Factor Authentication) where systems and services support it.

h) When using personal equipment, staff (students are out of scope) must:

- Ensure the device is enrolled in MS Company Portal\Intune.
- Ensure the device is up to date
- Ensure the device has Anti-virus installed and up to date
- Report to IT as soon as possible if the device is lost and contains any Hartpury data.

3. Consequences of Breach

In the event of a breach of this Acceptable Use Policy by a user, Hartpury may in its sole discretion:

a) restrict or terminate a user's right to use the network;
b) withdraw or remove any material uploaded by that User in contravention of this policy; or
c) where appropriate, disclose information to law enforcement agencies and take any legal action against a user for breach of this Policy, including but not limited to claiming all costs, fees and disbursements (including but not limited to legal fees) connected therewith.

In addition, where the user is also a member of the Hartpury community, Hartpury may take such action, disciplinary or otherwise as it deems appropriate and which is in accordance with Hartpury codes of conduct, policies and procedures.

4. Data Storage

As part of Hartpury's provision of IT facilities, students and staff Hartpury related data will be backed up, providing that data has been saved correctly and in the recommended locations. Student and staff data held on backups will not be recovered unless

- the creator of the original data makes the request and is currently a student or member of staff of Hartpury,
- the request has been made by a line manager.
- the request has been made by a tutor or lecturer of a student.
- the request has been made by a member of the Executive in relation to either an investigation of a breach of the Acceptable Use Policy or an investigation carried by an authorised external body such as the police.

5. Leaving Hartpury

Upon leaving Hartpury, user accounts (including all files and emails) will be deleted as per the guidance below.

Students

A student IT account and the data in the account is deleted 5 months after completion of the academic course attended by that student, as defined in Hartpury's student records system.

Students must transfer all their important personal files from their Hartpury file space before leaving Hartpury.

Students must change any logins to any external system where they have used Hartpury email addresses. Failure to do so may result in loss of access to these systems and inability to recover access.

If suspending attendance at Hartpury, computer user accounts will normally be suspended; files and file space will be preserved. On return, access will be reinstated.

Staff

A staff\contractor IT account and the data in the account is deleted in accordance with the Hartpury Information Retention and Disposal Policy.

Hartpury staff must obtain written approval from their line manager before they copy any Hartpury information from Hartpury systems. Removing any data that includes sensitive, internal or personal information will be considered a data breach.

Staff must change any logins to any external system where they have used Hartpury email addresses. Failure to do so may result in loss of access to these systems and inability to recover access.

If suspending attendance at Hartpury (e.g. sabbaticals, long term sick, maternity leave) computer user accounts will normally be suspended; files and file space will be preserved. On return, access will be reinstated.

6. Filtering and Monitoring

Keeping Children Safe in Education (September 2023) has seen a focus placed on the issue of filtering and monitoring in schools and colleges. As such Hartpury will ensure its filtering system blocks harmful and inappropriate content without unreasonably impacting teaching and learning. An active and well managed filtering system is an important part of providing a safe environment for students to learn. An effective filtering system needs to block internet access to harmful sites and inappropriate content. However, it should not unreasonably impact teaching and learning, or other aspects of Hartpury administration and it should not restrict students from learning how to assess and manage risk themselves.

Hartpury reserves the right to log and retain records of all electronic communications (web browsing activities, email exchange etc) between users of Hartpury IT and computing facilities and all external organizations for a period of no more than 18 months under the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000.

Use of Hartpury's digital systems (including e-mail, telephony systems and the Internet connectivity) is primarily for work-related purposes. Hartpury has the right to scan or monitor any and all aspects of its telephone and computer digital systems including https traffic that are made available to staff, students and visitors, and to monitor, intercept and/or record any communications including telephone, e-mail or Internet communications.

In addition, Hartpury wishes to make all staff, students and visitors aware that video surveillance is in operation for the protection of staff, students and visitors. Images are recorded for the purposes of public safety, crime prevention, detection and prosecution of offenders. See the relevant policy for more details.

7. Definitions

Hartpury network – all computing, telecommunication, and networking facilities provided by Hartpury, including cloud services, computing devices, connected to Hartpury's systems and services.

Member of Hartpury – a current member of staff or a student including those who have suspended their studies.

8. Related Policies

- Child Protection and Safeguarding Policy & Procedures
- Keeping Children Safe in Education (DfE statutory guidance)
- Staff Code of Conduct
- Student Code of Conduct
- Social Media Policy
- The JANET Acceptable use policy can be found here: https://community.jisc.ac.uk/library/acceptable-use-policy
- Password Policy
- Information Security Policy
- Hartpury Artificial Intelligence (AI) position statement

EQUALITY, DIVERSITY AND INCLUSION

As with all Hartpury policies and procedures, due care has been taken to ensure that this policy is appropriate to all members of staff and students regardless of their age, disability, ethnicity, gender, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sexual orientation and transgender status.

The policy will be applied fairly and consistently whilst upholding Hartpury's commitment to providing equality to all.

Hartpury is committed towards promoting positive mental health and aims to create a culture of support where staff and students can talk about mental health problems without the fear of stigma or discrimination.

APPROVAL & REVIEW CYCLE		
Reviewed By	Director of Continuous Improvement and Digital Services	April 2025
Approved By	Exec	April 2025
Interim-Review	No	-
Next Review Date		April 2026