HARTPURY

IT Acceptable Use Policy

Classification: Public
Author(s): Head of Information Technology
Approved by: Executive
Owner: Head of Information Technology
Issue date: 06/09/2020
Review date: 10/8/2021

Effective from	**September 2020**
Next review by	**August 2021**
Owned by	**Head of IT**
Reviewed by	**Executive**
Signed-off by	**Executive**

Revision History

Name	Date	Reason For Changes	Version
Matthew Reeve	1/5/19	Creation of new AUP	V1
Matthew Reeve	10/8/20	Review of AUP	V2

Introduction

It is the responsibility of all users of the Hartpury services to read and understand this policy. This policy may be updated from time to time, in order to comply with legal and policy requirements.

1.1 Purpose

This Acceptable Use Policy is intended to provide a framework for such use of Hartpury's I.T. resources. It should be interpreted such that it has the widest application and so as 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 appendix.

1.3 Scope

Members of Hartpury and all other 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 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, discriminatory, extremist or which has the potential to radicalise themselves or others;

3. unsolicited "nuisance" emails;

4. material which is subsequently used to facilitate harassment, bullying and/or victimisation of a member of Hartpury or a third party;

5. 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;

6. material with the intent to defraud or which is likely to deceive a third party;

7. material which advocates or promotes any unlawful act;

8. 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

9. material that brings the Hartpury into disrepute.

b) The Network 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 User's 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 Network is being used to access another network, any abuse of the acceptable use policy of that network will be regarded as unacceptable use of the Network.

e) Users shall 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;

- access or try to access data where the user knows or ought to know that they should have no access;

- carry out any hacking activities; or

- Intentionally or recklessly introduce any form of spyware, computer virus or other potentially malicious software.

- Use unencrypted removable media or unauthorised cloud storage.

f) Exemptions from Unacceptable Use: There are a number of legitimate academic activities that may be carried out using Hartpury's information systems that could be considered unacceptable use, as defined at 2a-e. 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.

Any potential research involving obscene or indecent material must always be discussed in advance with Hartpury's Designated Safeguarding Lead (or Deputy). If a user of the Hartpury Network believes they may have encountered breaches of any of the above, they should make this known to a member of the Safeguarding Team.

g) When using Hartpury computing facilities users MUST:

- log out of your account if you are leaving a computer 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.

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

Hartpury requires all students to store and backup their own work. A student IT account and the data contained in the IT account is deleted at the end of the longest running academic course attended by that student, as defined in Hartpury's student records system.   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, or 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 external body such as the police.

5 Leaving Hartpury

When you leave Hartpury your account and all files contained within it will be deleted. You must make all efforts to transfer important files from your Hartpury file space before you leave Hartpury.

If you suspend your attendance at Hartpury, your computer user account will normally be suspended and your files and file space will be preserved. On return access will be reinstated.

6 Monitoring

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.

Use of e-mail, telephony system and the Internet is primarily for work-related purposes. Hartpury has the right to monitor any and all aspects of its telephone and computer system 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.

To ensure compliance with this policy or for any other purpose authorised under the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, staff, students and visitors are hereby required to expressly consent to Hartpury doing so.

In addition, the College wishes to make all staff, students and visitors aware that Close Circuit Television (CCTV) is in operation for the protection of staff, students and visitors. Images are being monitored and recorded for the purposes of public safety, crime prevention, detection and prosecution of offenders.

7 Definitions

Hartpury Network – all computing, telecommunication, and networking facilities provided by Hartpury, with particular reference to all computing devices, either personal or Hartpury owned, connected to systems and services supplied.

8 Related Policies

- Child Protection and Safeguarding Policy & Procedures
- 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