`

DATA PROTECTION POLICY

INTRODUCTION

This policy relates to data protection, as outlined in the Data Protection Act 2018, and how data and information is managed at Hartpury University & Hartpury College (Hartpury).

PURPOSE

Data protection legislation, including the General Data Protection Regulation (GDPR) and the UK Data Protection Act (DPA) 2018 applies to all data and information relating to an identified or identifiable living individual. This is defined as personal data within data protection legislation.

Hartpury takes the protection of all personal data extremely seriously and is committed to a policy of protecting the rights and freedoms of individuals with respect to the processing of their personal data and information.

SCOPE

This Policy applies to all members of staff employed by Hartpury, including honorary staff/associates, contractors, hourly paid teachers and any students or interns who are carrying out work on behalf of, or in relation to their studies at Hartpury involving the handling personal data.

You have a crucial role to play in ensuring that Hartpury maintains the trust and confidence of the individuals about whom Hartpury processes personal data (including its own staff), complying with the Hartpury's legal obligations and protecting Hartpury's reputation. This Policy therefore sets out what Hartpury expects from you in this regard. Compliance with this Policy and the related policies and procedures is mandatory. Any breach of this Policy and any related policies and procedures may result in disciplinary action.

Hartpury holds and processes information about its current, past or prospective employees, prospective students, applicants, current students, alumni, research subjects, parents/carers or sponsors, suppliers and other third parties who are defined as data subjects within data protection legislation.

This Policy applies to all personal data that Hartpury processes regardless of the format or media on which the data are stored or who it relates to.

`

Hartpury processes personal information for a variety of reasons which it defines within its General Privacy Notice.

Examples of these purposes, but not limited to, include:

- Administration of the student application process
- Academic administration
- Managing Human Resources processes, such as applications, performance management, training and development
- Administration of financial aspects of an individual's relationship with Hartpury
- Management of use of facilities and participation in events
- Enabling effective communications with staff, students and parents/carers/sponsors
- Operation of security, disciplinary, complaint and quality assurance processes and arrangements
- Support of Health, Safety and Welfare requirements
- Production of statistics and research for internal and statutory reporting purposes.
- Fundraising and Marketing

OBJECTIVES

The aim of this policy to ensure that data is managed in line with data protection legal requirements and enable the maintenance of authentic, reliable and useable data and information, which is capable of supporting business functions and activities for as long as they are required. This will be achieved through the consolidation, establishment and continuous improvement of effective records management policies and procedures. This document outlines compliance and practice around the key principles of the DPA and GDPR legislation, as well as good practice in information management

PRINCIPLES

The GDPR is based on a set of core principles that Hartpury must observe and comply with at all times from the moment that personal data are collected until the moment that personal data are deleted or destroyed.

Anyone who processes personal data within Hartpury must comply with the principles of data protection. The Principles define how data can be legally processed regardless of the format or media used. Processing means any operation which is performed on personal data or sets of personal data, by automated or manual means such as collecting, recording, organising, storing, adapting, altering, consulting, using, disclosing, combining, restricting, erasing or destroying.

The principles of data protection state that personal data shall be:

a) processed lawfully, fairly and in a transparent manner in relation to the data subject;

`

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes (although certain other safeguards must be in place as defined within the GDPR);

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) accurate and, where necessary, kept up to date;

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods when processed only for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of appropriate measures to protect the rights and freedoms of data subjects;

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Additionally, Hartpury must ensure that:

1. Personal data are not transferred outside of the EEA (which includes the use of any website or application that is hosted on servers located outside of EEA) to another country without appropriate safeguards being in place.

2. Hartpury allows data subjects to exercise their rights in relation to their personal data (listed below under Data Subject Rights)

Hartpury shall be responsible for, and be able to demonstrate, compliance with data protection legislation.

Roles and Responsibilities

Hartpury, as data controller (ICO Registration number: Z1591909), is responsible for overall compliance with data protection legislation and meeting the accountability and transparency obligations within the legislation. Key roles include Data Protection Officer, Information Governance Manager and Senior Managers (roles defined in the Information Governance policy), however all staff have a responsibility to ensure they process personal data in accordance with the data protection principles and other requirements of data protection legislation.

`

PROCEDURES

Information Asset Owners

The Information Asset Owner will be a member of staff who manages an information collection or data asset and has the power to make decisions about how that data is managed.

Information Asset Owners will work with the Information Governance Manager to disseminate guidance and information relating to data protection and good information handling practices, as well as suspected incident or breach reporting to the DPO and maintaining the Information Asset registers to demonstrate accountability in relation to data protection.

Record of processing

Information Asset Owners will be responsible for recording data/information assets within Hartpury's Information Asset Register(s) and for maintaining this register.

Data Protection Impact Assessments

A Data Protection Impact Assessment (DPIA), is a process to help identify and minimise the data protection risks involved in projects, processes and activities involving the processing of personal data.

DPIAs are required for processing likely to result in high risk to the individuals and their personal data, and where significantly altered processes and new technologies are involved.

All major data processing activities, especially new processing of personal data or adaptations of existing methods of processing, should be risk assessed using the Hartpury's Data Protection Impact Assessment process by the Information Asset Owner to ensure that the proposed processing complies with the requirements of data protection and risks are identified and effectively managed.

Templates and guidance provided by the Information Governance Manager should be used to complete the Data Protection Impact Assessment. DPIAs needed to be reviewed by the DPO and IT services.

Data Subject Rights

Hartpury will comply with all data subject rights, as appropriate in relation to the processing it undertakes.

These rights are:

- Transparency of processing
- Right of access to personal data
- Right of rectification of inaccurate personal data
- Right of erasure
- Right to restriction of processing
- Right to data portability

`

- Right to object to processing where it is processed in the following way:
    - for direct marketing purposes
    - for scientific/historical/research/statistical purposes
    - based on legitimate interest grounds
    - necessary for the performance of a task carried out in the public interest
- Right to object to automated individual decision making, including profiling

Transparency of processing

Details of the use of personal data by Hartpury can be found in Hartpury's General Privacy Notice.

Subject Access Requests

The Data Protection Act 2018 entitles any individual whose data is processed by Hartpury to request a copy of that data; this is known as a data subject access request (SAR). The right of the individual under the Act is to be told by us whether we or someone else on our behalf is processing your personal data and if so, to be given a description of the personal data, the purposes for which they are being processed and the likely recipients and sources of that personal data. They are also entitled to receive a copy of this personal data.

Any person can exercise this right by submitting a Subject Access Request form, available on our website here. Any formal subject access request must be responded to within the 30 calendar days, or appropriate additional timescale as laid down by data protection legislation.

Data sharing

All sharing of personal data with third parties will be subject to the appropriate controls as laid out in data protection legislation.

Repeated or ongoing data sharing arrangements will be covered by an appropriate data sharing or processor agreement and/or where appropriate by contract to comply with this policy. New agreements will be subject to a Data Protection Impact Assessment (DPIA) to assess risk and establish appropriate controls and measures around sharing data. These should be completed by the Information Asset Owner (new business owner of the process or line of business system).

Use of personal data within research

Where research involves the processing of personal data, the Chief or Principal Investigator/Researcher will be considered to be the relevant Information Asset Owner for the data.

All requirements of this policy relating to processing of personal data should be adhered to alongside Hartpury's research good practice requirements as outlined in the Intellectual Property Policy.

Use of personal data for research purposes will be subject to the appropriate safeguards as specified within the data protection legislation. In particular, personal data should be limited to the minimum amount of data which is reasonably required to achieve the desired academic objectives. Wherever possible, personal data should be anonymised or pseudonymised so that the data subjects cannot be identified.

`

Accountability and Record Keeping

Hartpury is responsible for and must be able to demonstrate compliance with the data protection principles and Hartpury's other obligations under the GDPR. This is known as the 'accountability principle'. Hartpury will ensure that it has adequate resources, systems and processes in place to demonstrate compliance with Hartpury s obligations including:

- appointing a suitably qualified and experienced Data Protection Officer (DPO) and providing them with adequate support and resource

- ensuring that at the time of deciding how Hartpury will process personal data, and throughout its processing, implementing appropriate technical and organisational measures that are designed to ensure compliance with the data protection principles (known as 'Data Protection by Design')

- ensuring that, by default, only personal data that are necessary for each specific purpose are processed both in relation to the nature, extent and volume of such personal data, the period of storage and the accessibility of the personal data (known as 'Data Protection by Default')

- ensuring that where any intended processing presents a high risk to the rights and freedoms of data subjects, Hartpury has carried out an assessment of those risks and is taking steps to mitigate those risks, by undertaking a 'Data Protection Impact Assessment'

- integrating data protection into Hartpury internal documents, privacy policies and fair processing notices

- offering training Hartpury staff on the GDPR, this policy and Hartpury's related policies and procedures, and maintaining a record of training completion by members of staff

- regularly monitoring the measures implemented by Hartpury to ensure they are effective Hartpury will keep records of all its processing activities in accordance with the GDPR requirements.

Staff must ensure that they have undertaken the prescribed training or consulted guidance provided by Hartpury and, where staff are responsible for other members of staff, that they have done so.

Managers must further review all the systems and processes under their control to ensure that they comply with Hartpury's obligations under this policy.

Staff must ensure that they observe and comply with all policies and guidance which form Hartpury's Information Governance Framework.

`

GOVERNANCE REQUIREMENTS

Implementation / Communication Plan
This policy is communicated to all staff as part of Hartpury's induction and general policy review process.

Exceptions to this Policy
There are no exceptions to this policy. Data Protection Legislation requires that all processing of personal data within Hartpury be subject to an appropriate policy.

REFERENCE TO OTHER DOCUMENTS

Hartpury General Privacy Notice
Subject Access Request form
Information Governance Policy
Data Protection Guidelines
Data Breach Reporting Policy/Procedure
IT Acceptable Use Policy
Intellectual Property Policy

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 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. If any employee feels that this or any other policy does not meet this aim, please contact the HR Department.

Hartpury is committed towards promoting positive mental health by working towards the MINDFUL EMPLOYER Charter. Hartpury aims to create a culture of support within the workplace where employees can talk about mental health problems without the fear of stigma or discrimination.

APPROVAL AND REVIEW CYCLE

This policy and specific subsidiary information governance and security policies will be annually reviewed by the Information Governance team to ensure that it remains appropriate in the light of any relevant changes to the law, Hartpury policies, contractual obligations, technological developments and emerging threats.

Date Last Approved	January 2022
Policy Owner	Information Governance Group
Approving Committee	Executive
Status	Apporoved
Effective from	Jan 2022
Next Review Date	January 2024