HUMAN RESOURCES POLICY AND PROCEDURE

DATA PROTECTION POLICY

1.0 Introduction

1.1 Hertford Regional College (HRC) is committed to being transparent about how it collects and uses the personal data of its workforce, and to meeting its data protection obligations. This policy sets out the college's commitment to data protection, and individual rights and obligations in relation to personal data.

1.2 This policy applies to the personal data of job applicants, employees, workers, contractors, volunteers, interns, apprentices and former employees, referred to as HR-related personal data. This policy does not apply to the personal data of clients or other personal data processed for business purposes.

1.3 HRC has appointed Olive Oliver – Assosciate Director as the person with responsibility for data protection compliance within the college. She can be contacted at ooliver@hrc.ac.uk. Questions about this policy, or requests for further information, should be directed to her.

2 Definitions

"Personal data" is any information that relates to a living individual who can be identified from that information. Processing is any use that is made of data, including collecting, storing, amending, disclosing or destroying it.

"Special categories of personal data" means information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and genetic and biometric data.

"Criminal records data" means information about an individual's criminal convictions and offences, and information relating to criminal allegations and proceedings.

3 Data protection principles

3.1 HRC processes HR-related personal data in accordance with the following data protection principles:

- The college processes personal data lawfully, fairly and in a transparent manner.
- The college collects personal data only for specified, explicit and legitimate purposes.
- The college processes personal data only where it is adequate, relevant and limited to what is necessary for the purposes of processing.
- The college keeps accurate personal data and takes all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay.
- The college keeps personal data only for the period necessary for processing.
- The college adopts appropriate measures to make sure that personal data is secure, and protected against unauthorised or unlawful processing, and accidental loss, destruction or damage.

3.2 The college tells individuals the reasons for processing their personal data, how it uses such data and the legal basis for processing in its privacy notices. It will not process personal data of individuals for other reasons. Where the college relies on its legitimate interests as the basis for processing data, it will carry out an assessment to ensure that those interests are not overridden by the rights and freedoms of individuals.

3.3 Where the college processes special categories of personal data or criminal records data to perform obligations or to exercise rights in employment law, this is done in accordance with a policy on special categories of data and criminal records data.

3.3 The college will update HR-related personal data promptly if an individual advises that his/her information has changed or is inaccurate.

3.4 Personal data gathered during the employment, worker, contractor or volunteer relationship, or apprenticeship or internship is held in the individual's personnel file (in hard copy or electronic format, or both), and on HR systems. The periods for which the college holds HR-related personal data are contained in its privacy notices to individuals.

3.5 The college keeps a record of its processing activities in respect of HR-related personal data in accordance with the requirements of the General Data Protection Regulation (GDPR).

4 Individual rights

4.1 As a data subject, individuals have a number of rights in relation to their personal data.

4.2 Subject access requests

Individuals have the right to make a subject access request. If an individual makes a subject access request, the college will tell him/her:

- whether or not his/her data is processed and if so why, the categories of personal data concerned and the source of the data if it is not collected from the individual;
- to whom his/her data is or may be disclosed, including to recipients located outside the European Economic Area (EEA) and the safeguards that apply to such transfers;
- for how long his/her personal data is stored (or how that period is decided);
- his/her rights to rectification or erasure of data, or to restrict or object to processing;
- his/her right to complain to the Information Commissioner if he/she thinks the college has failed to comply with his/her data protection rights; and
- whether or not the college carries out automated decision-making and the logic involved in any such decision-making.

4.3 The college will also provide the individual with a copy of the personal data undergoing processing. This will normally be in electronic form if the individual has made a request electronically, unless he/she agrees otherwise.

If the individual wants additional copies, the college will charge a fee, which will be based on the administrative cost to the college of providing the additional copies

4.4 To make a subject access request, the individual should send the request to Olive Olive (ooliver@hrc.ac.uk) and use the college's Subject Access request specified in Appendix A – also available on Staff Net. In some cases, the college may need to ask for proof of identification before the request can be processed. The college will inform the individual if it needs to verify his/her identity and the documents it requires.

4.5 The college will normally respond to a request within a period of one month from the date it is received. In some cases, such as where the college processes large amounts of the individual's data, it may respond within three months of the date the request is received. The college will write to the individual within one month of receiving the original request to tell him/her if this is the case.

4.6 If a subject access request is manifestly unfounded or excessive, the college is not obliged to comply with it. Alternatively, the college can agree to respond but will charge a fee, which will be based on the administrative cost of responding to the request. A subject access request is likely to be manifestly unfounded or excessive where it repeats a request to which the college has already responded. If an individual submits a request that is unfounded or excessive, the college will notify him/her that this is the case and whether or not it will respond to it.

5. Other rights

5.1 Individuals have a number of other rights in relation to their personal data. They can require the college to:

- rectify inaccurate data;
- stop processing or erase data that is no longer necessary for the purposes of processing;
- stop processing or erase data if the individual's interests override the college's legitimate grounds for processing data (where the college relies on its legitimate interests as a reason for processing data);
- stop processing or erase data if processing is unlawful; and
- stop processing data for a period if data is inaccurate or if there is a dispute about whether or not the individual's interests override the college's legitimate grounds for processing data.

To ask the college to take any of these steps, the individual should send the request to Olive Oliver (ooliver@hrc.ac.uk.

6 Data security

The college takes the security of HR-related personal data seriously. The college has internal policies and controls in place to protect personal data against loss, accidental destruction, misuse or disclosure, and to ensure that data is not accessed, except by employees in the proper performance of their duties.

All data is backed up and replicated between 2 sites for Disaster Recovery purposes and kept for at least 1 year. All areas of data are protected by security access restrictions either by user or by security groups. Access to these group is only provided if approval is given by the manager of that area, these calls are logged on the IT Helpdesk so a record of access is kept. All user account passwords expire after 90 days, any staff that leave the organisation their account expires on their leave date.

Where the college engages third parties to process personal data on its behalf, such parties do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

7 Impact assessments

7.1 Some of the processing that the college carries out may result in risks to privacy. Where processing would result in a high risk to individual's rights and freedoms, the college will carry out a data protection impact assessment to determine the necessity and proportionality of processing. This will include considering the purposes for which the activity is carried out, the risks for individuals and the measures that can be put in place to mitigate those risks.

8. Data breaches

8.1 If the college discovers that there has been a breach of HR-related personal data that poses a risk to the rights and freedoms of individuals, it will report it to the Information Commissioner within 72 hours of discovery. The college will record all data breaches regardless of their effect.

8.2 If the breach is likely to result in a high risk to the rights and freedoms of individuals, it will tell affected individuals that there has been a breach and provide them with information about its likely consequences and the mitigation measures it has taken.]

9. International data transfers

9.1 The college will not transfer HR-related personal data to countries outside the EEA.

10. Individual responsibilities

10.1 Individuals are responsible for helping the college keep their personal data up to date. Individuals should let the college know if data provided to the college changes, for example if an individual moves house or changes his/her bank details.

10.2 Individuals may have access to the personal data of other individuals and of our customers and clients in the course of their employment, contract, volunteer period, internship or apprenticeship. Where this is the case, the college relies on individuals to help meet its data protection obligations to staff and to customers and clients.

10.3 Individuals who have access to personal data are required:

- to access only data that they have authority to access and only for authorised purposes;
- not to disclose data except to individuals (whether inside or outside the college) who have appropriate authorisation;
- to keep data secure (for example by complying with rules on access to premises, computer access, including password protection, and secure file storage and destruction);
- not to remove personal data, or devices containing or that can be used to access personal data, from the college's premises without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device;
- not to store personal data on local drives or on personal devices that are used for work purposes; and
- to report data breaches of which they become aware to the data protection officer immediately.

10.4 Further details about the college's security procedures can be found in its data security policy.

10.5 Failing to observe these requirements may amount to a disciplinary offence, which will be dealt with under the college's disciplinary procedure. Significant or deliberate breaches of this policy, such as accessing employee or customer data without authorisation or a legitimate reason to do so, may constitute gross misconduct and could lead to dismissal without notice.

11. Training

11.1 The college will provide training to all individuals about their data protection responsibilities as part of the induction process and at regular intervals thereafter.

11.2 Individuals whose roles require regular access to personal data, or who are responsible for implementing this policy or responding to subject access requests under this policy, will receive additional training to help them understand their duties and how to comply with them.

Date of document establishment and initial approval	14 May 2018
Version number	Version 1
Approving body	Board of Corporation – approved 11.7.18
Designated owner	Director of HR and Corporate Development
Linked policies and procedures	Employee Privacy Notice Data Secruity Policy
Date of last review	N/a
Date of next review	May 2020

Appendix A

Subject Access Request form (Staff)

Name:
Daytime telephone number:
Email:
Address:
Employee number:
By completing this form, you are making a request under the General Data Protection Regulation (GDPR) for information held about you, by the organisation, that you are eligible to receive.
Required information (and any relevant dates):
By signing below, you indicate that you are the individual named above. Hertford Regional College cannot accept requests regarding your personal data from anyone else, including family members. We may need to contact you for further identifying information before responding to your request. You confirm that you are the individual named and will fully indemnify us for all losses, cost and expenses if you are not. Please return this form to the HR Services Department, Ware Campus, London Road, Ware, Herts SG12 9JF or email hr@hrc.ac.uk Please allow 28 days for a reply.
Data subject's signature:
Date: