The College of Animal Welfare

DATA PROTECTION POLICY AND PROCEDURE

INTRODUCTION

The College of Animal Welfare is committed to preserving the privacy of its learners, employees and other stakeholders, and to complying with the EU General Data Protection Regulation (GDPR). To achieve this commitment information about our learners, employees and other clients and contacts must be collected and used fairly, stored safely and not unlawfully disclosed to any other person.

It is College policy to make as much information public as possible and in particular, the following information will be available to the public.

- Names of the College Advisory Committee Members
- Photographs of key staff (i.e. members of the SMT and other managers) with the consent of the individuals
- List of staff.
- Learner performance data.
- Data Protection Officer contact details

PRINCIPLES

The College, its staff and others who process or use any personal information must ensure that they follow the data protection principles set out in article 5 of the GDPR. These are that personal data shall:

- Be processed lawfully, fairly and in a transparent manner in relation to individuals.
- Be 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 purpose.
- Be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- Be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
- 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 insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.

- Be 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.

The College will not release staff or learner data to third parties except to relevant statutory bodies. In all other circumstances, the College will obtain the consent of the individuals concerned before releasing personal data.

Data security

The organisation takes the security of personal data seriously. The organisation 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

RESPONSIBILITIES

College Advisory Board
The CAW Advisory Board are responsible for the oversight of this policy.

The Principal and Senior Managers
It will be the responsibility of the Principal all managers to ensure the implementation and compliance with the policy and for ensuring that it is communicated to all staff.

Data Protection Controller
The nominated Data Protection Controller for the College is the Vice Principal Corporate Services – who has operational responsibility for the implementation of this policy and for the reporting of any breaches.

Managers
All managers are responsible for ensuring that staff and learners are aware of and comply with this policy.

All Staff
Staff are responsible for ensuring that any personal data, which they hold, is kept securely and that personal information is not disclosed in any way and to any unauthorised third party. No information pertaining to a learners personal data must be kept on their personal computers.

Learners and Staff
Learners and staff are responsible for ensuring that all personal data provided to the College is accurate and up to date.

COMPLIANCE
Failure to comply with the GDPR policy and procedure will result in disciplinary action.

REVIEW
This policy and related procedures will be reviewed and issued on an annual basis.

GDPR PROCEDURE

1. INTRODUCTION

The College needs to keep certain information about its employees, learners and other users to allow us to monitor recruitment, attendance, performance, achievements and health and safety. It is also necessary to process information so that staff can be recruited and paid, courses organised and to comply with legal obligations to funding bodies and government. To comply with the law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. To do this, the College must comply with the Data Protection Principles, which are set out in the GDPR. In summary, these state that personal data shall:

- Be processed lawfully, fairly and in a transparent manner in relation to individuals.
- Be 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 purpose.
- Be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- Be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
- 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 insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.
- Be 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.
- The controller shall be responsible for, and be able to demonstrate, compliance with the principles.

The College and all staff or others who process or use any personal information must ensure that they follow these principles at all times.

The College tells individuals the reasons for processing their personal data, how it uses such data and the legal basis for processing. It will not process personal data of individuals for other reasons.

Personal data gathered during the employment, contractor or apprenticeship is held in the individual's personnel file and on HR systems. The periods for which the organisation holds HR-related personal data are contained in the below addendum.

The organisation keeps a record of its processing activities in respect of HR-related personal data in accordance with the requirements of the GDPR.

The College will keep a register of staff authorised to access and process learner and staff data and these members of staff will be asked to agree a confidentiality statement at induction.

2. RESPONSIBILITIES OF STAFF

2.1 Information about Yourself

All staff are responsible for:

- Checking that any information they provide to the College in connection with their employment is accurate and up-to-date.
- Informing the College of any changes to information, which they have provided, i.e. change of address.
- Informing the College of any errors or changes. The College cannot be held responsible for any errors unless the staff member has informed us of them.

2.2 Information about Other People

All staff must comply with the following guidelines:

All staff will process data about individuals on a regular basis, when marking registers, writing reports or references, or as part of a pastoral or academic supervisory role. The College will ensure through registration procedures, that all individuals give their consent to this type of processing, and are notified of the categories of processing, as required by the GDPR. The information that staff deal with on a day-to-day basis will be 'standard' and will cover categories such as:

- General personal details such as name and address.
- Details about class attendance, course work marks and grades and associated comments.
- Notes of personal supervision, including matters about behaviour and discipline.

Information about an individual's physical or mental health; sexual orientation; political or religious views; trade union membership or ethnicity or race is sensitive and can only be collected and processed with consent.

All staff have a duty to make sure that they comply with the data protection principles, which are set out in the staff handbook and the College Data Protection Policy. In particular, staff must ensure that records are:

- Accurate;
- Up-to-date;
- Fair;
- Kept and disposed of safely, and in accordance with the College policy.

The College will designate staff in the relevant area as 'authorised staff'. These staff are the only staff authorised to access data that is:

- Not standard data; or
- Sensitive data.

The only exception to this will be if a non-authorised member is satisfied that the requirement to access the data meets the below criteria and can demonstrate that the processing of the data is necessary:

- In the best interests of the individual or staff member, or a third person, or the College AND
- He or she has either informed the authorised person of this, or has been unable to do so and processing is urgent and necessary in all the circumstances.
- This should only happen in very limited circumstances. e.g., an individual is injured and unconscious and in need of medical attention or a member of staff tells the hospital that the individual is pregnant or a Jehovah's Witness.

Authorised staff will be responsible for ensuring that all personal data is kept securely. In particular staff must ensure that personal data is:

- Put away in lockable storage
- Not left on unattended photocopiers, printers, desks or tables.
- Unattended ICT equipment should not be accessible to other users.
- ICT equipment used off-site must be password-protected.
- Data files on any removable media (e.g. USB stick) or email attachments used off-site containing personal data must be password-protected.
- Paper records containing personal data must be shredded where appropriate.

Staff must not disclose personal data to any individual, unless for normal academic or pastoral purposes, without authorisation or agreement from the data controller, or in line with the College policy.

Staff shall not disclose personal data to any other staff member except with the authorisation or agreement of the designated data controller, or in line with the College policy.

Before processing any personal data, all staff should consider the following.

- Do you really need to record the information?
- Is the information 'sensitive'?
- If it is sensitive, do you have the data subject's express consent?
- Has the individual been told that this type of data will be processed?
- Are you authorised to collect/store/process the data?
- If yes, have you checked with the data subject that the data is accurate?
- Are you sure that the data is secure?
- If you do not have the data subject's consent to process, are you satisfied that it is in the best interests of the individual or the safety of others to collect and retain the data?
- Has the person been given the option to opt out?

3. RIGHTS TO ACCESS INFORMATION

Staff, individuals and other users of the College have the right to access any personal data that is being kept about them either on computer or in certain files. Any person who wishes to exercise this right should complete the College Standard Request Form for Access to Data and send it to the data controller. (Appendix 1), also located on the VLE and Cawpers.

The College will provide a copy of the information free of charge. However, the College can charge a 'reasonable fee' when a request is manifestly unfounded or excessive and to comply with requests for further copies of the same information.

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 organisation has failed to comply with his/her data protection rights; and
- whether or not the organisation carries out automated decision-making and the logic involved in any such decision-making.

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.

The College aims to comply with requests for access to personal information as quickly as possible. The College aims to ensure that it is provided within one month of receipt (in line with legislation). Where requests are complex or numerous this may take longer. In such cases, the reason for delay will be explained in writing, within 10 days of the initial request, to the data subject making the request.

4. SUBJECT CONSENT

In many cases, the College can only process personal data with the consent of the individual. In some cases, if the data is sensitive, **express consent** must be obtained. Agreement to the College processing some specified classes of personal data is a condition of acceptance of an individual onto any course, and a condition of employment for staff. This includes information about previous criminal convictions.

Some jobs or courses will bring the applicants into contact with children, including young people between the ages of 16 and 18. The College has a duty under the Children Act and other enactment to ensure that staff are suitable for any job offered. The College also has a duty of care to all staff and learners and must therefore make sure employees and those who use the College facilities do not pose a threat or danger to other users.

The College will also ask for information about particular health needs, such as allergies to particular forms of medication, or any conditions such as asthma or diabetes. The College will only use the information in the protection of the health and safety of the individual, but will need consent to process in the event of a medical emergency and for making arrangements for placing students in the workplace, for example.

Therefore, all prospective staff will be asked to sign either an appropriate HR form or an individual document regarding particular types of information when an offer of employment is made. A refusal to sign such documents may result in the offer being withdrawn.

Learners are required to agree to the College processing their data at the start of their course application process.

Other rights

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 the Vice Principal Corporate Services, lhsconfidential@caw.ac.uk

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.

CCTV, videos and photographs

Images of identifiable Individuals (Data Subjects) constitutes as processing personal information. This is completed in line with data protection principles.

CCTV - The CCTV Policy will be followed in relation to the use and purpose of CCTV monitoring across our various buildings. We will also set out the purposes for CCTV monitoring in our Privacy Notices.

Data Protection Impact Assessment – We will carry out a Data Protection Impact Assessment in accordance with data protection legislation and guidance from the ICO and other official agencies.

Photographs and non-CCTV recorded images will be taken for a variety of purposes, these will be outlined on our Privacy Notices and we will normally make it clear as to the purpose at the time the photograph/video is being captured. Where we do not have a legal or contractual basis for taking photographs or recording/videoing of students, staff and others we will obtain consent from the individual concerned (or person with legal responsibility/legal guardian if under the age of consent or the person is deemed not capable of giving consent). Precautions will be taken, as outlined in the Learner IT Acceptable Use Policy in relation to the taking and publishing photographs of students, in print, video or on the College website.

Data breaches

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

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.

Training

The College will provide training to all individuals about their data protection responsibilities as part of their induction process and ongoing training.

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.

5. THE DATA CONTROLLER AND THE DESIGNATED DATA USERS

The College as a corporate body is the data controller under the regulation, and the Managers therefore ultimately responsible for implementation. However, the designated data controller and data users will deal with day-to-day matters.

The nominated Data Protection Controller is the Vice Principal Corporate Services, whose contact details can be found on the College's VLE. In the event of the Vice Principal Corporate Services being unavailable, the nominated deputy for the Data Protection Controller is the Human Resources Manager.

The College's designated data users are the HR Manager who is responsible for all data relating to staff and the Vice Principal Student Services who is responsible for all data relating to learners and finance.

6. RETENTION OF DATA

Please see appendix 2 for the guidelines for the retention of personal data.

7. NOTIFICATION OF CHANGES TO THE PROCESSING OF PERSONAL DATA

The Data Protection Register for the College can be found on the ICO website www.ICO.org.uk.

Any changes will be reflected on Therefore and notified in the first instance on the College Intranet.

8. CONCLUSION

Compliance with the GDPR is the responsibility of all members of the College. Any breach of the data protection policy will lead to disciplinary action being taken, access to the College being withdrawn, or even a criminal prosecution. Any questions or concerns about the interpretation of this policy should be referred to your line manager.

APPENDIX 1

The College of Animal Welfare

STANDARD REQUEST FORM FOR ACCESS TO DATA

Name:

Daytime telephone number:

Email:

Address:

By completing this form, you are making a request under the General Data Protection Regulation (GDPR) for information held about you by the College that you are eligible to receive.

Required information (and any relevant dates):

Example: Emails in which I am identifiable sent between person A and person b from 1 January 2019 to 31st March 2019.

By signing below, you indicate that you are the individual named above. The 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 warrant 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: Vice Principal Corporate Services, lhsconfidential@caw.ac.uk

.

Please allow 28 days for a reply.

Data subject's signature:

Date:

APPENDIX 2

GUIDELINES FOR RETENTION OF PERSONAL DATA

Type of Data	Suggested Retention Period	Reason
Personnel files including training records and notes of disciplinary and grievance hearings.	6 years from the end of employment	References and potential litigation
Application forms/interview notes	12 months from the date of the interviews.	Time limits on litigation
Facts relating to redundancies where less than 20 redundancies	3 years from the date of redundancy	As above
Facts relating to redundancies where 20 or more redundancies	12 years from date of redundancies	Limitation Act 1980
Income Tax and NI returns, including correspondence with tax office	At least 3 years after the end of the financial year to which the records relate	Income Tax (Employment) Regulations 1993
Statutory Maternity Pay records and calculations	As Above	Statutory Maternity Pay (General) Regulations 1986
Statutory Sick Pay records and calculations	As Above	Statutory Sick Pay (General) Regulations 1982
Wages and Salary records	7 years	Taxes Management Act 1970
Accident books, and records and reports of accidents	3 years after the date of the last entry	RIDDOR 1985
Health records	During employment	Management of Health and Safety at Work Regulations
Health records where reason for termination of employment is connected with health, including stress related illness.	3 years	Limitation period for personal injury claims
Medical Records kept by reason of the Control of Substances Hazardous to Health Regulations 1994	40 years	COSHHR 1994
CCTV, Videos and photography	31 days	GDPR
Student records, including academic achievements, and conduct.	At least 6 years from the date the student leaves the College, in case of litigation for negligence, At least 10 years for personal and academic references, with the agreement of the student.	Limitation period for negligence.