Policy/procedure title	Data Protection Policy		
Review Cycle *Please specify	1 year	**Responsible Department**	Corporate Services
Procedure Owner *overall responsibility		Head of Governance	
Responsible Person (if different to above) *responsibility for communicating changes and staff training where appropriate			
Types of provision this procedure applies to: (delete as appropriate)	14-16 Study Programmes 19+ Apprenticeships Higher Education		

Revision Record		
Rev. No.	**Date of Issue**	**Details and purpose of Revision:**
1	01/052018	Review
2	26/04/2024	Feedback from OU compliance added and policy reformatted
3	07/04/2025	To separate data protection from retention so policy is stand alone

Equality Impact Assessment

Whenever a policy is reviewed or changed, it's impact assessment also must be updated. The Equality Act 2010 seeks to simplify discrimination law and introduced statutory duties to promote equality whereby The College of West Anglia must, in the exercise of its functions, pay due regard to the need to promote equality in relation to the protected characteristics.

Could any staff or students be adversely impacted by this policy/process? If yes give details and how this will be mitigated:

Date	**Action and Monitoring:**
April 2024	**None**
April 2025	**None**

E, D & I Statement

This procedure has been reviewed in line with the Equality Act 2010 which recognises the following categories of individual as Protected Characteristics: Age, Gender Reassignment., Marriage and Civil Partnership, Pregnancy and Maternity, Race, Religion and Belief, Sex (gender), Sexual Orientation and Disability. We will continue to monitor this procedure to ensure that it allows equal access and does not discriminate against any individual or group of people.

Contents

1 Introduction

1.1 The college is committed to protecting the rights and freedoms of data subjects (people) and the safe and secure processing of their personal data in accordance with Data Protection Legislation.

1.2 Data Protection legislation means the Data Protection Act 2018 (DPA2018), United Kingdom General Data Protection Regulation (UK GDPR), the Privacy and Electronic Communications (EU Directive) Regulations 2003, all the foregoing as amended from time to time, and any legislation implemented in connection with the aforementioned legislation.

1.3 Where data is processed by a controller or processor established in the European Union or comprises the data of people in the European Union, it also includes the EU General Data Protection regulations (EU GDPR). This includes any replacement legislation coming into effect from time to time.

1.4 The college holds personal data about its employees, students, suppliers, and other individuals for a variety of business purposes.

1.5 This policy sets out how the college seeks to protect personal data and ensure that our employees understand the rules governing their use of the personal data to which they have access during their work.

1.6 In particular, this policy requires staff to ensure that the Data Protection Officer (DPO) be consulted before any significant new data processing activity is initiated to ensure that relevant compliance steps are addressed.

1.7 The college leadership is fully committed to ensuring continued and effective implementation of this policy and expects all employees to share in this commitment. Any breach of this policy will be taken seriously and may result in disciplinary action.

2 Definitions

Business purposes	The purpose for which personal data may be used by the college: Personnel, administrative, financial, regulatory, payroll and business development purposes. *Business purposes include the following:* • *Compliance with our legal, regulatory and corporate*

	governance obligations and good practice • *Gathering information as part of investigations by regulatory bodies or in connection with legal processing or requests* • *Ensuring business policies are adhered to (such as policies covering email and internet use)* • *Operational reasons, such as recording transactions, training and quality control, ensuring the confidentiality of commercially sensitive information, security vetting, credit scoring and checking* • *Investigating complaints* • *Checking references, ensuring safe working practices, monitoring and managing staff access to systems and facilities and staff absences, administration and assessments* • *Monitoring staff conduct, disciplinary matters* • *Marketing our business* • *Improving services*
Personal data	'Personal data' means any information relating to an identified or identifiable person ('data subject'), an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person. *Personal data that the college may gather includes individuals' phone numbers, email addresses, educational background, financial and pay details, details of certificates and diplomas, education and skills, marital status, nationalities, job tiles, and CVs.*
Special Categories of personal data	Special categories of personal data include information about an individual's racial or ethnic origin, political

	opinions, religious or similar beliefs, trade union membership, physical or mental health or condition, criminal offences, or related proceedings, and genetic and biometric information – any use of special categories of personal data should be strictly controlled in accordance with this policy. *Special categories of personal data the college may gather includes employee health data, DBS checks, EDI profile data, and safeguarding records.*
Data controller	'Data controller' means the person or legal person, public authority, agency or other body which, alone or jointly with others determines the purposes and means of the processing or personal data; where the purposes and means of such processing are determined by law, the controller may be provided for in law.
Data processor	'Data processor' means a person or legal person, public authority, agency or other body, which processes person data on behalf of the controller.
Processing	'Processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Supervisory authority	This is the national body responsible for data protection. The supervisory authority for the college is the Information Commissioner's Office.

3 Scope

3.1 This policy applies to all processing of personal data whether:

- Wholly or partly by automated means (i.e., by computer, apps, or other digital system), or

- By other means (i.e., paper records) that form part of a filing system or are intended to form part of a filing system.

3.2 This policy applies to all staff and anyone else working on behalf of the college including contractors, who must be familiar with this policy and comply with its terms.

3.3 This policy supplements other college policies such as those relating to internet and email use. This policy may be amended with additional policies and guidelines from time to time.

Who is responsible for this policy?

3.4 The college Data Protection Officer (DPO) is responsible for the day-to-day implementation of this policy. Staff should contact the DPO for further information if necessary.

4 Purpose

4.1 The purpose of this policy is to also provide guidance on the Data Protection principles that apply when any personal data belonging to or provided by data subjects is collected, stored, or transmitted.

4.2 It is therefore imperative that all employees, and contractors, comply with the six Data Protection Principles, summarised below.

1) **Processed lawfully, fairly and in a transparent manner.**

   The College maintains up to date privacy notices to ensure individuals are fully informed about what personal data is being processed and why. Where Personal Data is provided by individuals, privacy information is provided to them at the time of collection. Where personal data is received about an individual from other sources, the College will provide the individual with a privacy notice about how the College will use their personal data as soon as reasonably possible and in any event within one month.

   The College identifies an appropriate lawful basis for processing as well as additional conditions to justify the processing of special category data and criminal offence data. As part of this the College maintains and publishes an Appropriate Policy Document.

2) **Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.**

The College ensures individuals are fully informed of the purpose of processing and records those purposes in privacy notices as well as wider documentation for accountability purposes. Should the purpose for which data is processed change over time, or a new purpose arise, the College will only proceed if the new purpose is compatible with the original purpose, the individual consents to the new purpose or a clear legal provision requires or allows the new processing in the public interest.

3) **Adequate, relevant and limited to what is necessary for the purposes for which it is being processed.**

The College ensures it only collects data that is actually needed for its specified purposes. We periodically review data and delete any data that is not needed to fulfil those purposes.

4) **Accurate and kept up to date, meaning that every reasonable step must be taken to ensure that personal data that is inaccurate is erased or rectified as soon as possible.**

The College ensures that data is recorded accurately and also records the source of the data provided. The College takes reasonable steps, having regard to the circumstances, the nature of the personal data and the purpose of processing, to ensure the accuracy of information.

The College recognises the importance of ensuring that personal data is amended, rectified, erased or its use restricted where this is appropriate under Data Protection legislation. The College has processes in place to respond to data subject rights requests appropriately and within statutory timescales.

5) **Kept for no longer than is necessary for the purposes for which it is being processed.**

The College maintains a Retention Schedule that sets out how long all data, including special category data, shall be retained for. This Schedule is kept under regular review. The College also reviews the data it holds at appropriate intervals as part of its regular review of the Record of Processing Activity held. When data

held is no longer needed for the purpose it was collected for, the College ensures it is deleted, destroyed or anonymised.

6) **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 has implemented appropriate technical measures to ensure the security of data processed. The College keeps its Information Security Policy, as well as Acceptable Use of IT Systems Policy, under regular review. The College ensures all staff undertake data protection training with annual refresher training.

4.3 In addition to complying with the above requirements the College also has to demonstrate in writing that it complies with them as part of its accountability obligations. The College has a number of policies and procedures in place, including this Policy and the documentation referred to in it, to ensure that the College can demonstrate its compliance. As part of this, we have published an Appropriate Policy in relation to our processing of Special Category and Criminal Offence Data, we keep our Record of Processing Activity under regular review. The College also ensures that Data Protection Impact Assessments are carried out for processing likely to result in a high risk to individuals' interests.

4.4 The college must ensure accountability and transparency in all use of personal data. Data Protection legislation obliges all staff to take a proactive approach to data protection.

4.5 In order to encourage best practice, and to avoid penalties from the Information Commissioner's office (ICO) all employees are required to read this policy, to treat others' personal data with due care and consideration and to ensure that the college is able to demonstrate compliance.

5 Procedures

Controlling vs processing data

5.1 The college is classified as a data controller (and a data processor). CWA is a data controller of its employee HR data but also for students' personal data we process as part of their educational journey through the college. In doing so, the college must

maintain its registration (data processing fee) with the Information Commissioner's Office.

5.2 The college is a data processor when CWA is contracted by a third- party organisation (e.g., Department for Education, DfE) o offer a service to data subjects and process their personal data for the data controller. In doing so the college must comply with contractual obligations and act only on the documented instructions of the data controller. If CWA at any point determine the purpose and means of processing without the instructions of the controller, the college shall be considered a data controller and therefore breach the contract with the controller and have the same liability as the controller.

5.3 As a data processor, the college must:

- Not use a sub-processor without the written authorisation of the data controller
- Co-operate fully with the ICO or other supervisory authority
- Ensure the security of the personal data
- Keep accurate records of processing activities
- Notify the controller of any personal data breaches

If there is doubt about how data is handled, contact the DPO for clarification.

Lawful basis for processing data

5.4 Where CWA is the data controller, personal data must be processed lawfully in accordance with individual's rights under the first principle. This means that a lawful basis for processing personal data must be established.

5.5 Staff must therefore ensure that any personal data they are responsible for managing or working with has a written lawful basis approved by the DPO.

5.6 If a lawful basis cannot be applied, our processing does not conform to the first principle and will be unlawful. Data subjects have the right to stop the processing of any personal data that has been unlawfully processed and have it erased.

5.7 At least one of the following basis must apply whenever personal data is processed

1) Consent

CWA holds recent, clear, explicit, and defined consent for the data subject's data to be processed for a specific purpose.

2) Contract

Processing is necessary to fulfil a contract with the individual or because they

have asked us to take steps prior to entering into a contract.

3) Legal obligation

Processing is necessary to meet a legal obligation (excluding a contract).

4) Vital interests

Processing is necessary to protect a person's life.

5) Public function

Processing is necessary to perform a task in the public interest or for an official function, and the task or function has a clear basis in law.

6) Legitimate interest

Processing is necessary for legitimate interest. This condition does not apply if there is a good reason to protect the individual's personal data which overrides the legitimate interest.

Deciding which condition to reply on

5.8 When assessing the lawful basis of processing, you must first establish that the processing is necessary to achieve the purpose. This means that processing must be a targeted, appropriate way of achieving a stated purpose. A lawful basis cannot be replied upon if the same purpose can be reasonably achieved by some other means that doesn't require the use of the personal data.

5.9 Only the minimum data required can be used to achieve the purpose (e.g., don't use a full date of birth if an age or age range will suffice).

5.10 Remember that more than one lawful basis may apply, and the best fit for the purpose should be relied upon, not what is easiest.

5.11 The following factors should be considered:

- What is the purpose for processing the data?
- Can it reasonably be done in a different way?
- Is there a choice as to whether or not to process the data?
- Who does the processing benefit?
- After selecting the lawful basis, is this the same as the lawful basis the data subject would expect?
- What is the impact of the processing on the individual?
- Are you in a position of power over them?
- Are they a vulnerable person?

- Would they be likely to object to the processing?
- Are you able to stop the processing at any time on request, and has this been factored into how this would be achieved?

5.12 The colleges commitment to the first principle requires the college to document this process and show that the lawful basis that best applies to each processing purpose has been considered, and full justification of these decisions made.

5.13 The college must also ensure that individuals whose data is being processed by the college are informed of the lawful basis for processing their data, as well as the intended purpose. This can be found in our Privacy Notice. A record of how individuals are to be informed, and a copy of the wording used for written communications must be kept. The colleges Privacy Notice can be found on our website at https://cwa.ac.uk/privacy-and-cookies.

5.14 If no other lawful basis applies, there may be the option to reply on Legitimate Interests. If this is the case a Legitimate Interests Assessment (LIA) must be undertaken and documented. The Data Protection Officer can assist in conducting and approving the assessment however, in most cases, Legitimate Interests is only likely to be a suitable lawful basis where the processing has little likelihood of affecting the rights or freedoms of the data subject.

6 Special Categories of Personal Data

What are special categories of personal data?

6.1 Previously known as sensitive personal data, special category data about an individual is more sensitive, so requires more protection. These types of personal data could create more significant risks to a person's fundamental rights and freedoms, for example by putting them at risk of unlawful discrimination. The special categories include information about an individual's:

- Race
- Ethnic origin
- Political opinions including party support or membership
- Religion
- Philosophy
- Trade union membership
- Genetics

- Biometrics (where used for ID purposes)
- Health (mental and physical)
- Sex life and sexual orientation

6.2 Whenever the college processes special category data, the college must identify a condition for processing as well as a lawful basis. The condition for processing special categories of personal data must comply with the law. If a condition for processing special categories of data cannot be identified, that processing activity must cease.

6.3 The college processes special categories of personal data so that we can comply with legal obligations such as health and safety at work and safeguarding.

Criminal Record Checks

6.4 Any criminal record check must be justified by law. Criminal record checks cannot be undertaken solely on the consent of the data subject. The college cannot keep a comprehensive register of criminal offence data. All data relating to criminal offences is considered to be special category of personal data and must be treated as such.

7 Responsibilities

7.1 College responsibilities

- Analysing and documenting the type of personal data the college holds
- Checking procedures to ensure that they cover all the rights of the individual
- Identifying the lawful basis for processing data
- Ensuring consent procedures are lawful
- Implementing and reviewing procedures to detect, report and investigate personal data breaches
- Storing data in safe and secure ways
- Assessing the risk that could be posed to individual rights and freedoms should data be comprised.

7.2 Staff responsibilities

- Fully understand your data protection obligations
- Check that any data processing activities you are dealing with comply with college policy and are justified
- Do not use data in any unlawful way

- Do not store data incorrectly, be careless with it or otherwise cause the college to breach data protection laws and college policies through your actions
- Comply with this policy at all times
- Raise any concerns, notify any breaches or errors, and report anything suspicious or contradictory to this policy and college obligations without delay. If in doubt, don't give it out, give the DPO a shout.

7.3 Responsibilities of the Data Protection Officer (DPO)

- Keep the board updated about data protection responsibilities, risks and issues
- Review all data protection procedures and policies on a regular basis
- Arrange data protection training and advice for all staff members
- Answer questions on data protection from staff, governors, and other stakeholders
- Respond to individuals such as students and staff who wish to know which data is being held about them by the college
- Checking and approving with third parties that handle the college's data and contracts or agreements regarding data processing
- Monitoring compliance with data protection legislation across the college.

7.4 Responsibilities of the Head of IT

- Ensuring all systems, services, software and equipment meet acceptable security standards
- Check and scan security hardware and software regularly to ensure it is functioning properly
- Research third party services, such as cloud services, the college is considering using to store or process data.

7.5 Responsibilities of the Head of Marketing and Communications

- Approve data protection statements attached to email and other marketing copy
- Assist the Data Protection Officer (DPO) with data protection queries from customers, target audiences or media outlets
- Coordinate with the Data Protection Officer (DPO) to ensure all marketing initiatives adhere to data protection laws and the college's Data Protection Policy.

7.6 Accuracy and relevance

The college will ensure that any personal data processed is accurate, adequate, relevant and not excessive, given the purpose for which it is obtained. The college will not process personal data obtained for one purpose for any unconnected purpose unless the individual concerned has agreed to this or would otherwise reasonably expect this.

7.7 If staff are not clear about the purpose for which data was collected but wish to use it, or intend to use it for another purpose, staff must seek approval from the Data Protection Officer (DPO) first who can confirm the purpose for which the data was collected and whether any new purpose is compatible. Where the proposed use is significantly different, involves combining data from different sources, or otherwise might have a significant impact on data subjects, the Data Protection Officer (DPO) may require a Data Protection Impact Assessment (DPIA) is undertaken.

7.8 Individuals may ask that the college corrects inaccurate personal data relating to them. If it is believed that the information is inaccurate it should be recorded that the accuracy of the information is disputed and the Data Protection Officer (DPO) informed.

7.9 Data Security

The college must keep personal data secure against loss or misuse. Where other organisations process personal data as a service on the college's behalf, the Data Protection Officer (DPO) will establish what, it any, additional specific data security arrangements need to be implemented in contracts with those third-party organisations.

7.10 Storing data securely

- In cases when data is stored on printed paper, it should be kept in a secure place where unauthorised personnel cannot access it
- Printed data should be shredded when it is no longer needed
- Data stored on a computer should be protected by strong passwords that are changed regularly. We encourage all staff to use strong 16-digit passwords
- Data stored on CDs or memory sticks (USB) must be encrypted or password protected and locked away securely when they are not being used
- Servers containing personal data must be kept in a secure location, away from general office space
- Data should be regularly backed up in line with the college's backup procedures

- Data should never be saved directly to mobile devices such as laptops, tablets or smartphones
- All servers containing sensitive data must be approved and protected by security software
- All possible technical measures must be put in place to keep data secure.

7.11 Data Retention

The college must retain data for no longer than necessary. What is necessary will depend on the circumstances of each case, taking into account the reasons that the personal data was obtained, but should be determined in a manner consistent with the colleges data retention guidelines. Consult with the Data Protection Officer (DPO) to ensure that an appropriate retention period is applied and the data included on the retention schedule is up to date.

7.12 Transferring data internationally

There are restrictions on international transfers of personal data. Personal data must not be transferred abroad, or anywhere outside of normal rules and procedures without the express permission from the Data Protection Officer (DPO).

8 Rights of Individuals

8.1 Individuals have rights to their data which the college must respect and comply with to the best of our ability. The college must ensure that individuals can exercise their rights in the following ways:

8.2 The right to be informed

Individuals have the right to be informed about the collection and use of their personal data. This is a key transparency requirement under GDPR. The college must provide individuals with information including; the purpose for processing their personal data, the retention period for that personal data, and who it will be shared with. This is called ‘privacy information’.

8.3 The right of Access

Individuals have the right to access the personal information that the college holds about them, by making a request. This is known as a ‘Subject Access Request’. An individual may appoint another person to act on their behalf in making a subject access request (SAR). When this happens, the college will need written evidence

that the individual concerned has authorised a third party to make the application and may also require further identification for the person making the request so that there is confidence of their identity. More detail can be found on this below.

8.4 The right to rectification

GDPR gives individuals the right to have personal data rectified. Personal data can be rectified if it is inaccurate or incomplete. The Data Protection Officer should be contacted if it is believed that the data held about an individual is inaccurate or out of date. On receiving a request for rectification, the college will take reasonable steps to determine the accuracy of the data held and will rectify the data if necessary. The processing of personal data in question will be restricted whilst this is being actioned.

8.5 The right to erasure (the right to be forgotten)

The right to erasure is also known as the 'right to be forgotten'. The broad principle underpinning this right is to enable an individual to request the deletion or removal of personal data where there is no compelling reason for its continued processing. The right to erasure does not provide an absolute 'right to be forgotten'. Individuals have a right to have personal data erased and to prevent processing in specific circumstances. The Data Protection Officer should be contacted in the event that an individual would like to exercise this right. The right to have their data erased and for processing to cease will occur under the following circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected and/or processed
- Where consent is withdrawn
- Where the individual objects to processing and there is no overriding legitimate interest for continuing the processing
- The personal data was unlawfully processed or otherwise breached data protection laws
- To comply with a legal obligation
- The processing relates to a child.

The Data Protection Officer (DPO) can refuse to comply with an erasure request where processing is necessary for the following reasons:

- To exercise the right of freedom of expression and information
- To comply with a legal obligation for the performance of a public interest task or exercise of official authority
- For public health purposes in the public interest
- For archiving purposes in the public interest, scientific research, historical research or statistical purposes
- The exercise of defence of legal claims.

If personal data that needs to be erased has been passed onto other parties or recipients, they must be contacted and informed of their obligation to erase the data. If the individual asks, the Data Protection Officer (DPO) must inform them of those recipients.

8.6 The right to restrict processing

Individuals have a right to 'block' or suppress processing of personal data. When processing is restricted, the college is permitted to store the personal data, but not to use it. The college is allowed to retain just enough information about the individual to ensure that the restriction is respected in future. This is not an absolute right and only applies in certain circumstances.

8.7 The right to data portability

The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hinderance to usability. Personal data can be provided to the individual directly or can be transmitted directly to another Data Controller on request. The right to portability only applies to personal data an individual has provided to the college, where the processing is based on the individual's consent or for the performance of a contract and when processing is carried out by automated means. If an individual requests for their personal data to be moved the college must provide the personal data in a structured, commonly used and machine-readable format. Open formats include CSV files.

8.8 The right to object

Individuals have the right to object to the college processing personal data in certain circumstances. Individuals will be informed of their right to object at the point of first communication if this applies and this will be detailed in the privacy notice for that first contact activity.

The college will stop processing personal data for direct marketing purposes as soon as it receives an objection. The college recognises that there are no exemptions or grounds to refuse and will cease processing unless:

- The college has legitimate grounds for processing which overrides the interests, rights and freedoms of the individual, or
- The processing relates to the establishment, exercise or defence of legal claims.

The college must always inform the individual of their right to object at the first point of communication, i.e., in the privacy notice and there must always be the option and ability for an individual to object online.

8.9 Rights related to automated decision-making including profiling

The college will only use automated decision making where the decision is necessary for the entry into or performance of a contract or is authorised by domestic law applicable to the college or is based on the individual's explicit consent. The college will provide individuals with information about the processing and about the ways in which they can request human intervention or challenge a decision. The college will carry out regular checks to ensure that its systems are working as intended.

The college may only carry out automated profiling or decision making that has a legal or similarly significant effect on an individual in the following circumstances:

- It is necessary for the entry into or the performance of a contract
- Based on the individual's explicit consent
- Otherwise authorised by law.

In these circumstances the college must:

- Give individuals detailed information about the automated processing
- Offer simple ways for them to request human intervention or challenge any decision about them

- Carry out regular checks and user testing to ensure that college systems are working as intended.

8.10 Response

The Data Protection Officer (DPO) must deal with rights requests without undue delay and within one calendar month. However, this can be extended by a further two months if the request is complex or a number of requests have been received by the individual. If an extension of time is necessary, the individual will be informed within one month of receiving their request and an explanation given as to why the extension is necessary.

9 Privacy Notices

When to supply a privacy notice

9.1 A privacy notice must be supplied at the time the data is obtained if obtained directly from the data subject. If the data is not obtained directly from the data subject, the privacy notice must be provided within a reasonable period of having obtained the data, which means within one month.

9.2 If the data is being used to communicate with the individual, then the privacy notice must be supplied at the latest when the first communication takes place.

9.3 If disclosure to another recipient is envisaged, then the privacy notice must be supplied prior to the data being disclosed.

What to include in a privacy notice

9.4 Privacy notices must be concise, transparent, intelligible and easily accessible. They are provided free of charge and must be written in clear and plain language, particularly if aimed at children.

9.5 The following information must be included in a privacy notice to all data subjects

- Identification and contact information of the data controller and the Data Protection Officer (DPO), if applicable
- The purpose of processing the data and the lawful basis for doing so
- The legitimate interests of the controller or third party, if applicable
- The right to withdraw consent at any time, if applicable
- The categories of personal data obtained (only for data not obtained directly from the data subject)

- Any recipient or categories of recipients of the personal data
- Detailed information of any transfers to third countries and safeguards in place
- The retention period of the data or the criteria used to determine the retention period, including details for the data disposal after the retention period
- The right to lodge a complaint with the ICO, and any internal complaints procedure(s)
- The source of the personal data, and whether it came from publicly available sources (only for data not obtained directly from the data subject)
- Any existence of automated decision making, including profiling and information about how those decisions are made, their significances and consequences to the data subject
- Whether the provision of personal data is part of a statutory or contractual requirement or obligation and possible consequences for any failure to provide the data (only for data obtained directly from the data subject).

9.6 At a minimum, all initial contacts with data subjects, or those which will require a new collection of or reason for processing data, must make reference to and link to the Privacy Notice on the college website https://cwa.ac.uk/privacy-and-cookies.

9.7 When collecting new data or processing it in a new way staff must seek advice from the Data Protection Officer (DPO).

9.8 Where you cannot easily link to the Privacy Notice on the college website when collecting data (for example for phone contacts) staff must consult with the Data Protection Officer (DPO) to agree how the Privacy Notice will be communicated (typically by follow-up email).

10 Data Subject Access Requests (DSARs)

10.1 Data Subject Access Requests

Individuals have the right to make a data subject access request. If an individual makes a subject access requires, the Data Protection Officer (DPO) will tell the data subject:

- Whether or not their 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 their data is or may be disclosed, including to recipients located outside the European Economic Area and the safeguards that apply to such transfers.

- For how long their personal data is stored.
- Their rights to rectification or erasure of data, or to restrict or object to processing.
- Their right to complain to the Information Commissioner if they thinks the college has failed to comply with their data protection rights, and
- Whether or not the college carried out automated decision-making and the logic involved in any such decision-making.

10.2 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 they agree otherwise.

10.3 To make a subject access request the individual should send the request to dpo@cwa.ac.uk. In some cases, the Data Protection Officer (DPO) may need to ask for proof of identification before the request can be processed. The Data Protection Officer (DPO) will inform the individual if it needs to verify their identity and the documentation required.

10.4 The Data Protection Officer (DPO) 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 request is complex, it may respond within three months of the date the request is received. The Data Protection Officer (DPO) will write to the individual within one month of receiving the original request to tell them if this is the case.

10.5 If an exemption applies, the college may refuse to comply with the request. Similarly, if a Data 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 Data 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 Data Protection Officer will notify the individual that this is the case and whether or not it they will respond to it. If the college refuses to comply with a request, it will notify the individual of the reasons why.

10.6 Data Portability requests

The Data Protection Officer (DPO) must provide the data requested in a structured, commonly used and machine-readable format. This would normally be a CSV file, although other formats are acceptable. The college must provide this data either to the individual who has requested it, or to the data controller they have requested it

be sent to. This must be done free of charge and without delay, and no later than one month. This can be extended to two months for complex or numerous requests, but the individual must be informed of the extension within one month.

11 Third Parties

11.1 As a data controller the college must have written contracts in place with any third party that is used. The contract must contain specific clauses which set out our and their liabilities, obligations and responsibilities.

11.2 As a data controller, the college must only appoint processors who can provide sufficient guarantees under the UK GDPR that the rights of data subjects will be respected and protected, and the personal data will be kept secure.

11.3 As a data processor, the college must only act on the documented instructions of a controller. The college acknowledges its responsibilities as a data processor under the UK GDPR and protects and respects the rights of data subjects.

Contracts

11.4 The colleges' contracts must comply with the minimum contractual requirements set out in the UK GDPR. College contracts with data controllers/processors must set out the subject matter and duration of the processing, the nature and stated purpose of the processing activities, the types of personal data and categories of data subject, and the obligations and rights of the controller/processor.

11.5 At a minimum, Data Processing Agreements with data controllers/processors must include terms that specify:

- The processor will act only on the written instructions of the controller
- Those involved in processing the data are subject to a duty of confidence
- Appropriate measures will be taken to ensure the security of the processing
- Sub-processors will only be engaged with the prior consent of the controller and under a written contract
- The controller will assist the processor in dealing with Data Subject Access Requests (DSAR) and allowing data subjects to exercise their tights under Data Protection legislation
- The processor will assist the controller in meetings its Data Protection legislation obligations in relation to the security of processing, notification of data breaches and performance of Data Protection Impact Assessments
- The processor will delete or return all personal data at the end of the contract

- The processor will submit to regular audits and inspections, and provide whatever information necessary for the controller and processor to meet their legal obligations.
- Nothing will be done by either the controller or processor to infringe Data Protection legislation.

11.6 In the event that staff are requested to share data with another organisation an agreement to do so must be in place. The Data Protection Officer (DPO) will draft the agreement for signature by both parties.

13 Audits, monitoring and training

13.1 **Data Audits**

Regular audits to manage and mitigate risks will be carried out. This includes information on what data is held, where it is stored, how it is use, who is responsible and any further regulations or retention timescales that may be relevant.

13.2 **Monitoring**

Staff must observe and adhere to this policy. The Data Protection Officer (DPO) has overall responsibility for this policy and will keep it under review and amend or change it as required. The Data Protection Officer (DPO) must be notified immediately of any breaches of this policy as staff are required to comply with this policy fully and at all times.

13.2 **Training**

Staff will receive adequate training on provisions of data protection law specific to their role. Staff must complete training as requested. If staff move role or responsibilities change, staff are responsible for requesting new data protection training relevant to the new role or responsibilities. The Data Protection Officer (DPO) can be contacted if staff require additional training on data protection matters.

14 Data Breaches

14.1 A Personal Data breach is defined as ‘a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.’ Whilst most Personal Data breaches happen as a result of action taken by a third party, they can also occur as a result of something someone internal does. They can be deliberate or accidental.

14.2 If the college discovers that there has been a breach of personal data that poses a risk to the rights and freedoms of individuals, it will report it to the Information Commissioners Office (ICO) within 72 hours of discovery. The college will record all data breaches and near misses regardless of their effect.

14.3 Any data breaches must be reported to the Data Protection Officer (DPO) immediately. A form for reporting data breaches can be found at Appendix 1.

14.4 If the breach is likely to result in a high risk to the rights and freedoms of individuals, the Data Protection Officer (DPO) will tell affected individuals that there has been a breach and provide them with information about its likely consequences and the mitigation measures being taken.

14.5 Staff have an obligation to report actual or potential data protection compliance failure. This allows the Data Protection Officer (DPO) to

- Investigate the failure and take remedial steps if necessary
- Maintain a log of compliance failures
- Notify the ICO of any compliance failures that are material either in their own right or as part of a pattern of failures.

14.6 Refer to the college's Data Breach Policy for more details.

15 Compliance

15.1 Compliance with the General Data Protection Regulation is the responsibility of everyone at the college. Any deliberate breach of the Data Protection Policy may lead to disciplinary action being taken, access to college facilities being withdrawn, or even a criminal prosecution. Any questions or concerns about the interpretation or operation of this policy should be taken up with the Data Protection Officer at dpo@cwa.ac.uk.

16 Related Policies

Special Category Date Appropriate Policy Document
Handling Data Protection Complaints
International Transfer Policy
Record of Processing Activities (RoPA)

Video Conferencing Policy

Data Protection Impact Assessment Policy

Data Sharing Policy

Data Subject Access Request Policy

Data Breach Policy

Data Retention and Destruction Policy

Appendix 1 Form for reporting a Data Breach

Please act promptly to report any data breaches. If you discover a data breach, please notify the Data Protection Officer immediately, complete this form and email it to dpo@cwa.ac.uk

Section 1: Notification of Data Breach	To be completed by the person reporting the incident
Date incident was discovered:	
Date(s) of incident:	
Place of incident:	
Name and Job Title of person reporting incident:	
Contact Details (email and extension number):	
Description of incident:	
Number of data subjects affected:	
Provide details of any personal data that has been placed at risk:	
Brief description of any containment action taken at the time of the discovery:	