Policy/procedure title	Data protection, Handling and Retention 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

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	**No Actions required HP**

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.

1 Purpose

1.1 The college is committed to being transparent about how it collects and uses the personal data of its workforce and students and to meeting its data protection obligations. This policy sets out the college's commitment to data protection together with 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, apprentices and former employes, referred to as HR-related personal data. This policy also applies to the personal data of students.

1.3 The college has appointed the Head of Governance as its Data Protection Officer. Their role is to inform and advise the college on its data protection obligations. Further detail about the responsibilities of the DPO are set out in section 13. The Head of Governance can be contacted at dpo@cwa.ac.uk. Questions about this policy, or requests for further information, should be directed to the Data Protection Officer.

2 Aims

The aims of the policy include the following:

- To explain how the College processes personal data, including sensitive personal data, in compliance with data protection legislation.
- To assist in meeting the College's accountability obligation by documenting its compliance measures as part of a wider suite of documentation in this area.
- To explain the responsibilities of staff under the General Data Protection Regulation and Data Protection Act (the UK's implementation of the GDPR).
- To explain the rights of individuals as data subjects.
- To explain how data breaches are handled.
- To provide information on the retention of data.

3 Introduction and Status of the Policy

3.1 The college needs to keep certain information about its employees, students and other stakeholders to allow it to monitor performance, achievements, and health and safety, for example. It is also necessary to process information so that staff can be recruited and paid, courses organised and legal obligations to funding bodies and

government complied with. 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 set out in the General Data Protection Regulation (often known as GDPR). These are detailed in section 5 below.

3.2 The college and all staff, or others who process or use any personal information, must ensure that they follow the data protection principles at all times. In order to ensure that this happens, the college has developed this Data Protection Policy alongside other related compliance documentation.

3.3 This policy does not form part of the formal contract of employment but is a condition of employment that employees will abide by the rules and policies made by the College of West Anglia from time to time. Any failures to follow the policy can therefore result in disciplinary proceedings, including dismissal.

3.4 Any member of staff, who considers that the policy has not been followed in respect of personal data about themselves, should raise the matter with the Data Protection Officer. If the matter is not resolved it should be raised as a formal grievance.

4 Definitions

4.1 Key definitions are detailed below:

- **Personal data**: is any information that relates to a living individual who can be identified directly or indirectly from that information or allows them to be identified in conjunction with other information that is held.

- **Processing** is any use that is made of data, including collecting, storing, amending, disclosing or destroying it.

- **Special categories of personal data:** is information that reveals an individual's

racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, physical or mental health, sex life or sexual orientation and biometric data.

- **Criminal records data**: is information about an individual's criminal convictions and offences and information relating to criminal allegations and proceedings.

- **Data Controller** – Any entity (for example company, organisation or person) that makes its own decisions about how it is going to collect and use Personal Data. A Data Controller is responsible for compliance with Data Protection Laws. Examples of Personal Data the College is the Data Controller of include employee details or information the College collects relating to students. The College will be viewed as a Data Controller of Personal Data if it decides what Personal Data the College is going to collect and how it will use it.

- **Data Processor** – Any entity (for example company, organisation or person) which accesses or uses Personal Data on the instruction of a Controller. A Data Processor is a third party that processes Personal Data on behalf of a Data Controller. This is usually as a result of the outsourcing of a service by the Data Controller or the provision of services by the Data Processor which involve access to or use of Personal Data.

5 Data Protection Principles

5.1 Data Protection law requires the College to comply with the following principles. These principles require personal data to be:

5.1.1 **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.

5.1.2 **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.

5.1.3 **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.

5.1.4 **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.

5.1.5 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.

5.1.6 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.

5.2 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.

6 Lawful Use of Personal Data

6.1 Processing personal data will not be lawful without a valid lawful basis. Documenting our processing activities and the lawful basis on which the processing is justified is also a key part of our accountability obligation under the legislation.

6.2 To ensure that our processing of personal data is lawful, the College has carefully assessed how it uses personal data and has identified one of the six grounds set out in Article 6 of the UK GDPR as a valid basis on which to process the data before the processing begins. Further information on the lawful bases can be found here.

6.3 Where the College processes special category or criminal offence data, it has to show that one of a number of additional conditions is met. These are set out in Article 9 of the UK GDPR. These additional conditions have also been assessed and the College has identified which are applicable in order to justify its processing of special category or criminal offence data. As part of this we have published an Appropriate Policy Document in relation to our processing of Special Category and Criminal Offence Data. Further information on the additional conditions for processing special category data can be found here.

6.4 Determining the correct legal basis for processing data can be difficult and more than one ground may be applicable. Please contact the Data Protection Officer on dpo@cwa.ac.uk for advice and guidance.

6.5 The College records all processing activities and the way in which it meets its compliance obligations. If the College changes how it uses personal data, the record will be updated and individuals be notified of the change as necessary. As such, if College personnel intend to change how they use personal data at any point they must notify the Data Protection Officer who will decide whether their intended use requires amendments to be made and any other measures which need to be taken.

7 Individual Rights

Data protection law gives individuals greater control over their personal data through several rights which the College strives to facilitate effectively.

Requests can be made verbally or in writing to dpo@cwa.ac.uk. As a member of college staff, if you receive a data subject rights request you should forward it to the DPO immediately and no later than within 24 hours of receipt. If the request is made verbally,

please obtain as much information as possible, including contact details for the data subject, and pass them immediately to the DPO.

The College must respond to data subject requests within one calendar month. It is possible to extend the time to respond by a further two months if the request is complex or if we have received a number of requests from the individual. The College will let the individual know that the time limit needs to be extended within one month of receiving the request and will explain the reasons for the extension.

Generally there is no fee for making a data subject rights request, however the College may charge a reasonable fee for the administrative costs of complying with a request if it is manifestly unfounded or excessive. Where the College charges a fee, we will contact the individual promptly to inform them. Please note that the College does not have to comply with the request until we have received the fee.

Some rights only apply in certain circumstances, depending on the lawful basis for processing. The College may refuse to comply with a request if an exemption applies or if a request is manifestly unfounded or excessive. Every request will be dealt with on a case by case basis. Further information on all data subject rights can be found at A guide to individual rights | ICO

If an individual has a complaint about the way in which their data subject rights request has been dealt with they should contact the Data Protection Officer at dpo@cwa.ac.uk..

If an individual remains dissatisfied they have the right to complain to the Information Commissioner's Office www.ico.org.uk

Please contact the Data Protection Officer at dpo@cwa.ac.uk if you wish to withdraw consent to processing.

7.1 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'.

7.2 The right of Access

Individuals have the right to access the personal information that the college holds about you, 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 we 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 we can be confident of their identity. More detail can be found on this below.

7.3 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. Please contact the DPO using the details below if you believe data we hold about you 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 we hold and will rectify the data if necessary. We will restrict processing the personal data in question while we do this.

7.4 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. If you would like more information, or would like to exercise this right, please contact the DPO, as set out below.

7.5 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 applies in certain circumstances.

7.6 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.

7.7 The right to object

Individuals have the right to object to the college processing personal data in certain circumstances. You will be informed of your 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.

7.8 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.

7.9 Subject Access Requests

Individuals have the right to make a subject access request. If an individual makes a subject access requires, the data protection officer 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 and the safeguards that apply to such transfers.
- For how long his/her personal data is stored.
- 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 carried 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.

To make a subject access request the individual should send the request to dpo@cwa.ac.uk. In some cases, the data protection officer may need to ask for proof of identification before the request can be processed. The data protection officer will inform the individual if it needs to verify his/her identity and the documentation required.

The procedure to be followed following a subject access request is illustrated at appendix 2. The procedure with regard to handling all other data subject rights requests can be found at appendix 3.

The Data Protection Officer 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 will write to the individual within one month of receiving the original request to tell him/her if this is the case.

If an exemption applies, the College may refuse to comply with the request. Similarly, 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 data protection officer will notify him/her 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.

8 Data Security

8.1 The college takes the security of personal data very seriously. The college has internal policies and controls, as well as appropriate security measures, 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.

8.2 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. Please see section 11 for more information on third party data processors.

9 Data Protection by Design and Default and Data Protection Impact Assessments

9.1 The concept of data protection by design seeks to ensure consideration of data protection issues at the outset and through the lifecycle of all processing activities. Data protection by default requires organisations to ensure that they only process the data that is necessary to achieve the specific purpose in hand. It links to the fundamental data protection principles of data minimisation and purpose limitation.

Data Protection Impact Assessments

9.2 Some of the processing that the college carries out may result in risks to privacy. DPIAs are a fundamental part of the concept of data protection by design in assessing the technical and organisational measures needed to ensure that processing complies with the data

protection principles. Where processing would result in a high risk to individual's rights and freedoms, the data protection officer will carry out a data protection impact assessment (DPIA) 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. As such a DPIA should be started as early as practical in the design of processing operations so that College can identify and fix problems with its proposed new process, product or service at an early stage, reducing the associated costs and damage to reputation, which might otherwise occur. Where a DPIA reveals a high risk which cannot be appropriately mitigated, the ICO must be consulted.

9.3 A DPIA must be completed where the use of Personal Data is likely to result in a high risk to the rights and freedoms of individuals. Alongside this trigger, there are certain specific circumstances in which a DPIA is mandatory, namely the following:

Under the GDPR a DPIA must be completed if the college plans to:

- Use systematic and extensive profiling with significant effects.
- Process special category or criminal offence data on a large scale, or,
- Systematically monitor publicly accessible places on a large scale.

9.4 The college is also required to complete a DPIA if it plans to:

- Use innovative technology (in combination with any of the criteria from the European guidelines).
- use profiling or special category data to decide on access to services.
- profile individuals on a large scale.
- process biometric data (in combination with any of the criteria from the European guidelines).
- process genetic data (in combination with any of the criteria from the European guidelines).
- match data or combine datasets from different sources.
- collect personal data from a source other than the individual without providing them with a privacy notice ('invisible processing') (in combination with any of the criteria from the European guidelines).

- track individuals' location or behaviour (in combination with any of the criteria from the European guidelines).
- profile children or target marketing or online services at them; or
- process data that might endanger the individual's physical health or safety in the event of a security breach.

9.5 It is important to note that consideration of data protection issues and risks is not just for new projects but may need to be addressed in relation to existing processing if the risks are sufficiently high and/or the way an activity is being carried out has changed. If you are unsure whether a DPIA is needed or have any questions about the process, please contact the DPO at dpo@cwa.ac.uk.

9.6 The College uses a DPIA template which is available here

10 Data Breaches

10.1 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.

10.2 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 Commissioner within 72 hours of discovery. The college will record all data breaches and near misses regardless of their effect.

10.3 Any data breaches must be reported to the Data Protection Officer immediately using the form at appendix 4. The DPO inbox is routinely monitored and in the absence of the DPO checking will be delegated.

10.4 If the breach is likely to result in a high risk to the rights and freedoms of individuals, the Data Protection Officer 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.

10.5 The College ensures that all college staff who have access to Personal Data are appropriately trained in data protection according to their role in order to reduce the likelihood of personal data misuse. This also ensures that staff are able to quickly recognise if a personal data breach has occurred to that swift action can be taken to mitigate the risks to data subjects and ensure compliance with the College's obligations in relation to data breaches.

10.6 The procedure to be followed upon notification of a data breach is provided for at appendix 5, demonstrated using a RACI matrix. This details who in the event of a breach is Responsible, Accountable, to be Consulted with, or Informed.

11 Appointing contractors who access the college's personal data

11.1 Under Data Protection legislation, the College may only appoint a contractor to process personal data on behalf of the College where the College has carried out sufficient due diligence and only where there are appropriate written contracts in place.

11.2 A Data Controller is considered as having appointed a Data Processor where it engages a third party to perform a service on its behalf, as part of which they will require or obtain access to that Controller's Personal Data. Where the College appoints a Data Processor in this way, it is the College which remains responsible for what happens to its personal data.

11.3 The legislation requires that a Data Controller must only use Processors who meet the requirements of the GDPR and protect the rights of individuals, which means that due diligence must be undertaken on both new and existing suppliers in relation to data protection requirements. Periodic audits must be carried out on Data Processors once appointed to ensure they continue to meet contractual requirements in relation to data protection.

11.4 The GDPR requires the contract with a Data Processor to contain the following obligations as a minimum:

- to only act on the written instructions of the Controller;
- to not export Personal Data without the Controller's instruction;
- to ensure staff are subject to confidentiality obligations;

- to take appropriate security measures;
- only engage sub-processors with the prior consent (specific or general) of the Controller and under a written contract;
- to keep the Personal Data secure and assist the Controller to do so;
- to assist with the notification of Data Breaches and Data Protection Impact Assessments;
- to assist with subject access/individuals' rights requests;
- to delete/return all Personal Data as requested at the end of the contract;
- submit to audits and provide information about the processing and to tell the Controller if any instruction is in breach of the GDPR or other EU or member state data protection law.

11.5 In addition, the contract should set out:

- the subject-matter and duration of the processing;
- the nature and purpose of the processing;
- the type of Personal Data and categories of individuals;
- and the obligations and rights of the Controller.

11.6 Any questions in relation to the College's use of Data Processors should be directed at the DPO at dpo@cwa.ac.uk.

12 International Data Transfers

12.1 From time to time the college may transfer your personal information to our service providers based outside of the UK. If the college does this your personal information will continue to be subject to one or more appropriate safeguards set out in the law. These might be the use of standard contractual clauses in a form approved by regulators, or having our suppliers sign up to an independent privacy scheme approved by regulators.

12.2 In order to ensure that the College is compliant with Data Protection legislation, College personnel must not export personal data unless it has been approved by the Data Protection Officer.

13 Roles and Responsibilities

13.1 Individual Responsibilities

13.1.1Individuals 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 a staff member moves house or changes his/her bank details, their employee self-service account should be updated.

13.1.2 Individuals may have access to the personal data of other individuals such as students. Where this is the case, the college relies on individuals to help meet its data protection obligations to staff and students.

13.1.3 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).
- 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 (Head of Governance) immediately.

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

13.2 Data Protection Officer (DPO)

13.2.1 The Data Protection Officer is responsible for:

- Advising on the implementation of this and related policies.
- Keeping information law policies and procedures under review and developing policies and guidance as required.
- Monitoring compliance with this and related policies, ensuring College data processing complies with data protection law.
- Providing advice and guidance on data protection and wider information law matters
- Investigating personal data breaches and notifying the ICO and data subjects as necessary.
- Responding to data subject rights requests (as well as requests under the Freedom of Information Act 2000 and the Environmental Information Regulations 2004) within statutory time frames and maintaining compliance logs.
- Maintaining the College's registration with the ICO and acting as point of contact with the ICO as necessary.
- Raising data protection awareness and ensuring data protection training requirements are complied with.

14 Training

14.1 The college will provide training to all individuals about their data protection responsibilities as part of the induction process.

14.2 Individuals whose roles require regular access to personal data will have a mandatory requirement to complete data protection training.

14.3 Staff are required to refresh their knowledge and understanding and will undertake mandatory training on an annual basis.

15 Conclusion

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 Documents

Appropriate Policy Document

Privacy Notices

Information Security

Data Protection Impact Assessment (DPIA) Template

Data Sharing Agreement

Appendix 1 Guidelines for Retention of Personal Data

Business Function	Dataset	Category	Minimum Retention Period	Authority/Justification
HR	Employment	Application forms and interview notes - (for unsuccessful candidates)	6 months to a year	Recommended practice (CIPD)
HR	Employment	Applications (successful)	6 months following end of probation (18 months)	Assess and verify suitability for role period – may retain useful data e.g. skills. Limitation incl. ED for unfair dismissal and discrimination claims etc
HR	Employment	Authorised absence records (annual leave, time off for dependents, jury service etc)	2 years from when the entry was made	Working Time Regulations 1998 Part II
HR	Employment	CCTV – relevant footage relating to an investigation or formal process	Extend normal retention period of CCTV for 6 months following a formal outcome or any appeal outcome	Recommended practice (ICO). Limitation incl. EC for unfair dismissal and discrimination claims etc
HR	Employment	Collective Agreements	6 years after ending	Limitation Act 1980 – limitation for breach of contract and negligence
HR	Employment	Contracts, offer letters and variations (including any flexible working outcome)	6 years following end of employment	Limitation Act 1980 – limitation for breach of contract
HR	Employment	Criminal Record (DBS) Checks and Disclosures (e.g. DBS Certificate)	6 years following end of employment	Limitation Act 1980 – limitation for negligence (made by Public etc)
HR	Employment	Capability and disciplinary documents (substantiated)	2 years following the issue of the warning	TUPE 2006. Case law permitting expired warnings to be referred to (but no built upon). Unreasonably to refer back after 2 years.
HR	Employment	Driving licence (if required for the post)	Duration of driving on College business + 3 years	Limitation Act 1980 – 3year limitation for negligence for a known act/incident
HR	Employment	Driving offences	Remove once the conviction is 'spent' unless subject to exemptions	Rehabilitation of Offenders Act 1974
HR	Employment	Drug and alcohol testing records	6 years from a positive result	Tribunal limitation incl. EC for breach of contract and discrimination claims etc.
HR	Employment	Drug and alcohol testing records	6 months from a negative result	Tribunal limitation incl. EC for breach of contract and discrimination claims etc.
HR	Employment	Flexible working request documentation	18 months following outcome (including any appeal outcome)	12month statutory embargo on a further request plus 6 month tribunal limitation incl. EC for auto-unfair dismissal and discrimination claims etc.

HR	Employment	Grievance documents	6 months following end of employment	Limitation incl. EC for 'last straw' constructive dismissal and discrimination claims etc
HR	Employment	Investigations – no case to answer	6 months following conclusion	Limitation incl. EC discrimination claims etc
HR	Employment	Maternity medical records	3 years after the end of the tax year in which the maternity period ends	The Statutory Maternity Pay (General) Regulations 1986 as amended
HR	Employment	Medical capability documents and records incl. OH reports	6 months following end of employment	Equality Act 2010, Limitation incl. EC for unfair dismissal and discrimination claims etc.
HR	Employment	Monitoring (e.g. vehicle trackers)	6 months rolling unless there is an overriding reason or on-going relevance of the record	Recommended practice (ICO)
HR	Employment	Qualifications	6 years following end of employment	Limitation Act 1980 – limitation for negligence (made by public etc)
HR	Employment	Right to work checks	Two years after employment	Recommended practice (Home Office)
HR	Employment	Redundancy details, calculations of payments and refunds	6 years from the date of redundancy	Recommended practice (CIPD) & Limitation Act 1980
HR	Employment	Redundancy – documentation	6 years following end of redundancy	Limitation Act 1980
HR	Employment	References received for employment	6 months following end of probation period (18 months)	Assess and verify suitability for role. Limitation incl. EC for unfair dismissal and discrimination claims etc. Also consider any insurance requirements, regulatory or supervisory obligations e.g. GMC, NMC, CQC, FCA
HR	Employment	References issued for employment	1 year	Defamation Act 1996 1year limitation in respect of any shared comments
HR	Employment	References and correspondence that may produce legal affects (mortgage, loan, etc)	3 years following issue	Limitation Act 1980 – limitation for negligence when immediately aware
HR	Employment	Sickness records and unauthorised absence records	6 months following end of employment - Pseudonymise where feasible	Limitation incl. EC for unfair dismissal and discrimination claims etc.
HR	Employment	Sickness and injury records (work related) (other than those listed under Health and Safety)	15 years	3 years for personal injury claim or 15 years for negligence (in respect of latent damage) Limitation Act 1980
HR	Employment	Whistleblowing reports and documents linked to an investigation which is partially or wholly substantiated.	6 months following the outcome of the report or any remedial action taken because of the report	Public Interest Disclosure Act 1998 ('PIDA 1998') Employment Rights Act 1996

HR	Employment	Whistleblowing – documents linked to an entirely unsubstantiated claim	Remove any personal data immediately	Recommended practice (IAPP)
HR	Employment	College Health Policies	12 years after final cessation of benefit	
HR	Employment	Records documenting the management of individual organisation restructuring processes	Completion of process + 5 years	
Finance	Finance	Accounting records	6 years + 1 current	Section 221 of the Companies Act 1985 as modified by the Companies Acts 1989 and 2006
Finance	Finance	Expense Accounts	6 years + 1 current	Companies Act 1985, section 222 as modified by the Companies Act 1989 and 2006
Finance	Finance	Income tax records and correspondence with HMRC	6 years + 1 current	The Income Tax (Employments) Regulations 1993 (SI 1993/744) as amended
Finance	Finance	Inland revenue/HMRC approvals	Permanently	Recommended practice (CIPD)
Finance	Payroll	National minimum wage records	6 years + 1 current	National Minimum Wage Act 1998
Finance	Payroll	Statutory Maternity Pay records, calculations, certificates (Mat B1's) and leave	6 years + 1 current	The Statutory Maternity Pay (General) Regulations 1986 as amended and Maternity & Paternal Leave Regulations 1999
Finance	Payroll	Statutory Adoption Pay records, calculations, matching certificates and leave	6 years + 1 current	Maternity & Parental Leave Regulations 1999
Finance	Payroll	Statutory Paternity Pay records, calculations and leave	6 years + 1 current	Maternity & Parental Leave Regulations 1999
Finance	Payroll	Statutory Shared Parental Pay records calculations, certificates (Mat B1's) notices and leave	6 years + 1 current	Maternity & Parental Leave Regulations 1999
Finance	Payroll	Wage/salary records (also overtime, bonuses, expenses)	6 years + 1 current	Taxes Management Act 1970
Finance	Payroll	Pension scheme investment policies	12 years from the ending of any benefit payable under the policy however no information should ever be retained unless it is a necessary consequence of the funding	Recommended practice (ICO)
Finance	Payroll	Pension records	6 years after the end of the tax year to which they relate – Reg.18 of The Registered Pension Schemes (Provision of Information) Regulations 2006	12 years after the benefit ceases. Avoid access unless required. Recommended practice (ICO)

Finance	Payroll	Retirement Benefits Schemes - records of notifiable events	6 years from the end of the scheme year in which the event took place	The Retirement Benefits Schemes (Information Powers) Regulations 1995
Finance	Payroll	Private medical	Avoid access unless required as part of making a reasonable adjustment etc	Recommended practice (ICO)
Finance	Payroll	Working time: Timesheets, overtime records and other documents relating to working time	6 years + 1 current	Working Time Regulations 1998 Part II
IT	IT	Proxy, Web, authentication, remote access & firewall logs	2 years +	Longer retention periods are required for high value data sources that can be used to identify the impact of new and existing persistent threats over typical attach timescales
IT	IT	Email, IDS, antivirus, database and network infrastructure logs	6 months to 1 year	While valuable these data sources are often coupled with active alerting facilities that can be notified to the security teams of incidents as they are being detected
IT	IT	Host process execution and file access	4 weeks to 6 months	Depending on the usage, host logging can create large numbers of events that are mainly used for verification after an intrusion has been discovered
IT	IT	Email accounts	2 years after employment ends	
Health and Safety	Employment	Professional insurance (including insurance for driving on business)	6 years following end of employment	Limitation Act 1980 – limitation for negligence (made by public etc.) Also consider any insurance requirements, regulatory or supervisory obligations e.g. GMC, NMC, CQC, FCA
Health and Safety	Employment	Driving licence (if required for the post)	Duration of driving on College business + 3 years	Limitation Act 1980 – 3year limitation for negligence for a known act/incident
Health and Safety	Employment	Driving offences	Remove once the conviction is ‘spent’ unless subject to exemptions	Rehabilitation of Offenders Act 1974
Health and Safety	Health and Safety	Accident/Incident books, records and reports	Adult: date of incident + 7 years Children: DOB of child + 25 years	The Reporting of Injuries, Diseases and Dangerous Oc currences Regulations 1995 (RIDDOR) (SI 1995/3163) as amended, and max. 15 years for negligence (in respect of latent damage) Limitation Act 1980
Health and Safety	Health and Safety	Enforcement/prosecutions under health and safety regulations and records of consultations with safety representatives and committees	Indefinitely	Recommended practice (CIPD)
Health and Safety	Health and Safety	First aid training	6 years after employment ends	Health and Safety (First-Aid) Regulations 1981

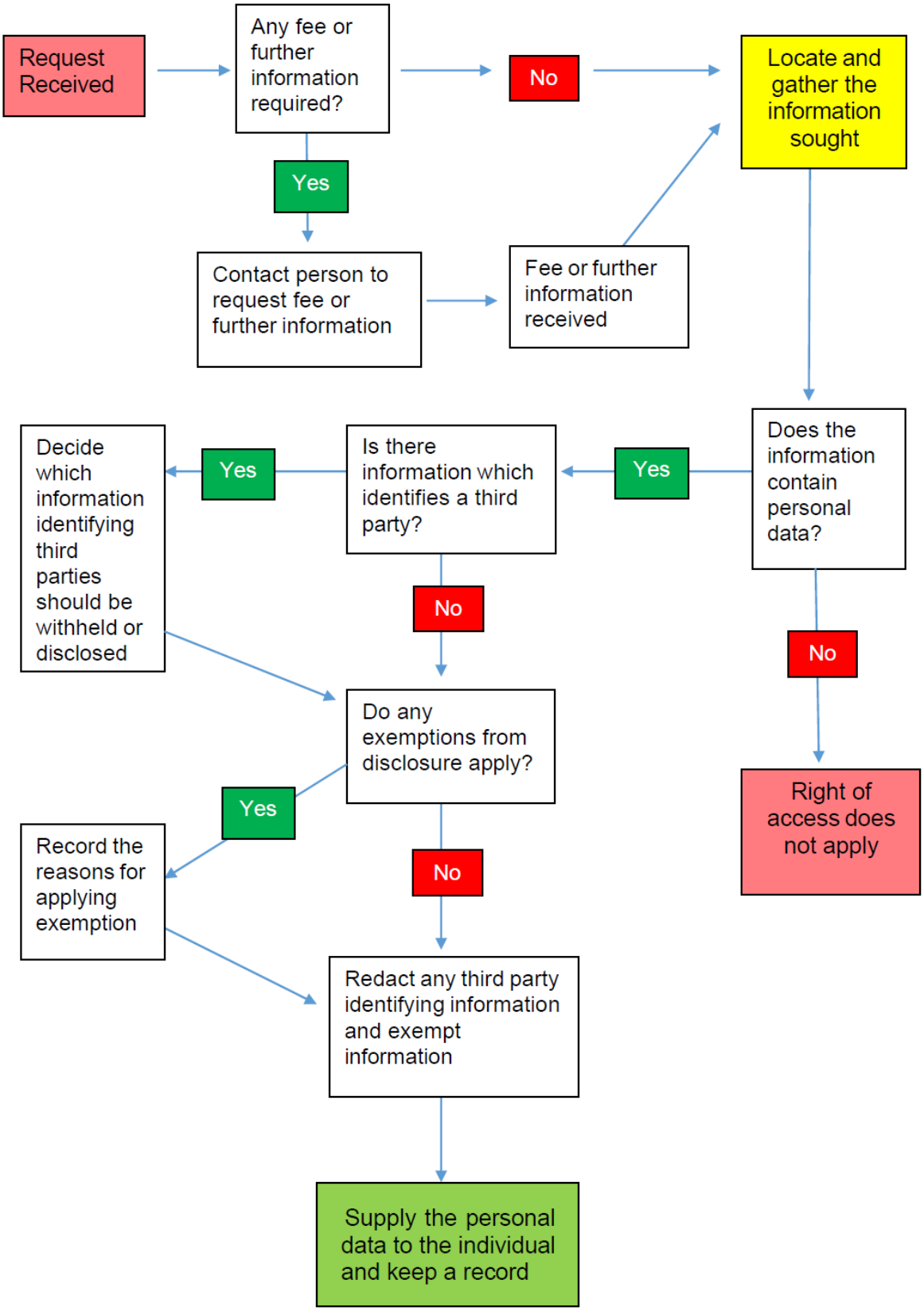
Health and Safety	Health and Safety	Fire Marshal training	6 years after employment ends	Fire Precautions (Workplace) Regulations 1997
Health and Safety	Health and Safety	H&S representatives training	5 years after employment ends	Health & Safety (Consultation with employees) Regulations 1996
Health and Safety	Health and Safety	H&S training - employees	5 years after employment ends	H&S Information for Employees Regulation 1989
Health and Safety	Health and Safety	Health records made in connection with health surveillance (according to HSE)	At least 40 years	Recommended practice (HSE) The Control of Substances Hazardous to Health Regulations 1999 and 2002
Health and Safety	Health and Safety	Medical records under the Control of Asbestos at Work Regulations: medical records containing details of employees exposed to asbestos	Medical records – At least 40 years from the date of the last entry; Medical examination certificates - 4 years from the date of issue	The Control of Asbestos at Work Regulations 2002 and the Control of Asbestos Regulations 2012
Health and Safety	Health and Safety	Medical records and details of biological tests under the Control of Lead at Work Regulations	At least 40 years from the date of the last entry	Control of Lead at Work Regulations 2002
Health and Safety	Health and Safety	Medical records as specified by the Control of Substances Hazardous to Health Regulations (COSHH)	At least 40 years from the date of the last entry if person is identifiable and the record represents exposure, otherwise at least 5 years	The Control of Substances Hazardous to Health Regulations 1999 and 2002
Health and Safety	Health and Safety	Medical records under the Ionising Radiations Regulations 1999	Until the person reaches 75 years of age, but in any event for at least 50 years	The Ionising Radiations Regulations 1999
Health and Safety	Health and Safety	Records of tests and examinations of control systems and protective equipment under the Control of Substances Hazardous to Health Regulations (COSHH)	5 years from the date on which the tests were carried out	The Control of Substances Hazardous to Health Regulations 1999 and 2002
Health and Safety	Health and Safety	Risk assessments (COSHH, Fire etc)	Whilst relevant + 6 years thereafter	HSE Risk Management
Health and Safety	Health and Safety	Statutory and regulatory training	6 years after employment ends	Limitation Act 1980
Health and Safety	Health and Safety	Medical records (general)	Recommended for 12 years	
Health and Safety	Health and Safety	PEEPS assessments - Accessibility	Closure + 12 years	
Health and Safety	Health and Safety	V1 and V2 Trips/Visits Forms	6 Years	

Health and Safety	Health and Safety	RIDDOR Reports	Indefinitely	Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 2013
Health and Safety	Health and Safety	DSE Assessments	Whilst relevant and 6 years thereafter	HSE Risk Management
Estates	Facilities Management	Buildings, compliance certificates/reports (lifts, LEV, electrical, gas, water etc)	6 years	
Estates	Facilities Management	Equipment compliance maintenance certificates/reports (PAT, hoists, cookers, fridges etc)	6 years	
Company	Legal	Subject Access Request Letters	1 year following completion of a request	May charge a fee for repeat copies. May be unreasonable to charge a fee after 12 months
Company	Legal	Contracts executed under seal	12 years after expiry	
Company	Policy	Complaints procedure	10 years	
Company	Policy	Complaints correspondence	10 years	
Estates	Procurement	Contracts with customer, suppliers, agents or others	6 years after expiry or contract completion	
Estates	Procurement	Rental & hire purchase agreements	6 years after expiration of agreement	
Estates	Procurement	Licensing agreements	6 years after expiration of agreement	
Estates	Procurement	Signed contracts	6 years after expiration of contract	
Estates	Procurement	Tendering – unsuccessful tender documents	3 years from date of award of contract	
Estates	Procurement	Tendering – successful tender documents	6 years	
Estates	Procurement	Tendering contract award letter	3 years from date of award of contract	
Estates	Procurement	Tendering – signed contract	6 years after expiration of contract	
Estates	Procurement	Supplier Contact Details	Permanently	
Company	Insurance	Public & Product liability	Permanently	
Company	Insurance	Employers liability policies	Statuary min 40 years recommend permanently	
Company	Insurance	Sundry insurance policies and insurance schedules	Until claims under policy are barred or 3 years after policy lapses whichever is longer	
Company	Insurance	Group personal accident policies	12 years after final cessation of benefit	

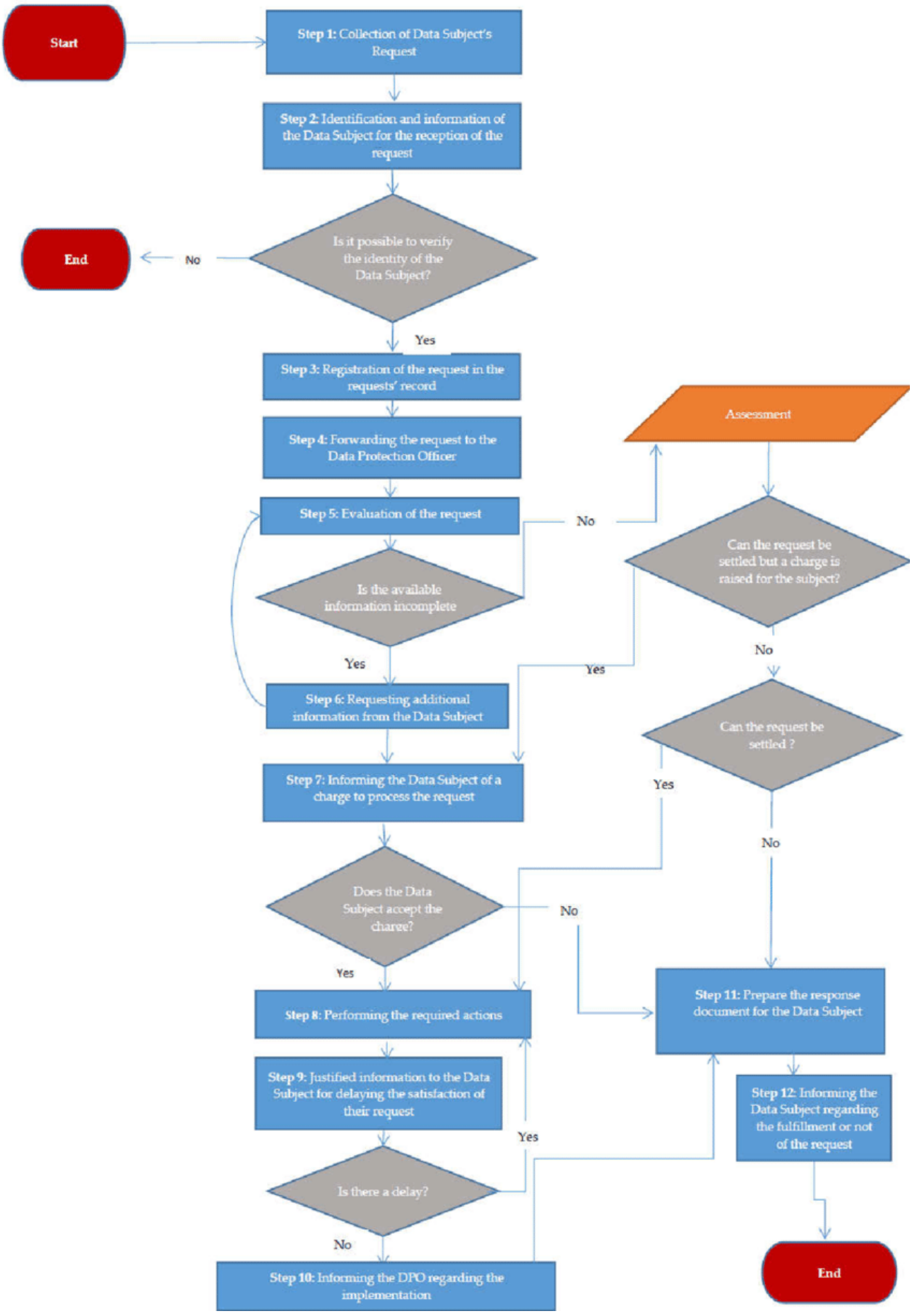
Governance	Corporate Management	Instrument and Articles of Government	Life of Institution	
Governance	Corporation	Records documenting the establishment and development of the governance structure	Life of Institution	
Governance	Corporation	Records documenting the appointment of members of the Corporation and its Committees	Termination/expiration of term of office + 6 years	
Governance	Corporation	Records of the provision of training and development for members of the Corporation and its Committees	Current year + 3 years	
Governance	Corporation	Register of Interests of Members of the Corporation and Senior Staff	Termination/expiration of term of office + 6 years	
Governance	Corporation	Records documenting the organisation of meetings (calendars, schedules etc) of the Corporation and its Committees	Current year + 1	
Governance	Corporation	Minutes documenting the conduct and proceedings of meetings of the Corporation and its Committees	Current year + 50 years	
Governance	Corporation	Records documenting the development and establishment of Terms of Reference for the Committees of the Corporation	Life of Committee	
Governance	Corporation	Records documenting the appointment and designation of Senior Post Holders	Termination/expiration of appointment + 5 years	
Governance	Corporation	Records documenting the development of the College's Strategic Plan	Superseded + 10 years	
Governance	Corporation	Records containing reports on the College's performance against its Strategic Plan	Current academic year + 10 years	
Governance	Corporation	Records documenting the conduct and results of audits and reviews of the Strategic Planning process(es) and responses to the results	Current academic year = 5 years	
Governance	Risk Management	Records documenting the development and establishment of the College's Risk Management Policy and Procedures	Current year + 10	
Governance	Risk Management	Records documenting the conduct and results of audits and reviews of the risk management function, and responses to the results	Current year + 5 years	
Governance	Risk Management	Risk Register	Superseded + 1 year	

Governance	Quality	Records documenting the development and establishment of the College's Self-Assessment Report	Superseded + 5 years	
Governance	Quality	Records documenting the conduct and results of quality audits, and action taken to address issues raised	Completion of Audit + 3 years	
Governance	Corporation	Quality Assurance records	12 years	
Safeguarding	Students	Child protection registers	26 years	
Safeguarding	Students	Secondary school files transferred to College	DOB of pupil + 25 years	
Safeguarding	Students	Special Education Needs files	DOB of pupil + 25 years	
Safeguarding	Students	Statement maintained under The Education Act1996 - Section 324	DOB + 30 years	
Safeguarding	Students	Proposed statement or amended statement	DOB + 30 years	
Safeguarding	Students	Advice and information to parents regarding educational needs	Closure + 12 years	
Students	Students	ESFA Learner files (all ages), including certificates	Six years from financial year end after end of course or until 31/12/2030 if ESF funded provision	Legal requirement by the European Social Fund, European Court of Auditors can audit up to 31/12/2030
Students	Students	Correspondence relating to authorised absence and issues	Date of absence + 2 years	
Students	Students	Exam results - public	Year of examination + 6 years	
Students	Students	Exam results - internal	Current year + 5 years	
Reception	Reception	Visitor book	Current + 2 years	

Appendix 2 Subject Access Request Procedure



Appendix 3 Procedure for handling other data subject rights requests



Appendix 4 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:	

Appendix 5 Incident and Breach Reporting - (RACI Matrix)

Incident & Breach Reporting - RACI Matrix

R	**RESPONSIBLE** Person responsible for completing the assigned deliverable
A	**ACCOUNTABLE** Ultimate Owner, Accountable for final decision
C	**CONSULTED** Person consulted before action or decision taken
I	**INFORMED** Person informed after action or decision taken

		Preparation																														
		Preparation			Detection & Notification				Assessment							Eradication & Notification				Post-incident Activity												
Project Participants		Define stakeholders	Define scope, definitions & classifications	Build Incident Response team	Incident intake	Triage & Classification: determine if PII information included	Declare a privacy breach and notify and convene IR team	Identify affected systems	Assess the impact of the breach	Determine whether specialised forensic experts are required	Perform forensic analysis	Escalate report to the ICO	Compile list of impacted parties who need to be contacted (internal)	Draft and agree on communicaiton plan based on findings	Update IR team	Remove any remaining threat	Action agreed comms plan (external)	Assign resources to recover any lost IT, business or operational functionality	Restore service	Prepare final incident report and submit to IR team	Update RACI	Provide refresher training to staff as required	Report to Senior Executives/Board	Update breach register
JB	DPL - Data Protection Officer	R A	R A	R A	R A	R A	R A	R A	R A	R	R A	C I	R A	R A	R A	R A	R A	R A	R A	R A	R A	A	R A	R A
RP	Data and Funding Performance	C	C	I	C I		I	C				I	C	I	I	R	I	C	I	I				
RT	IT Services Manager	C	C	I	I		I	C				I	C	I	I	R	I	C	I	I				
MB	Marketing Manager	C	C	C			I	I	C I			I		R C	I	I	R		I	I				
JB	Corporation (Governors)																						I	I
PH	Funding Bodies (dependent upon nature of Breach)																							
JH	Human Resources	I	I	C			I		I				I		I	I				I		R		
LC	Admissions and Business Support Manager	I	I	C			I						I		I	I				I				
LC	Reception and Customer Services Co-ordinator	I	I	C			I		I			I	I	I	I	I	I			I				
GG	Health and Safety	I	I	C			I						I		I	I				I				
JB/LJ	Third Party Processors (dependent upon nature of Breach)																							