Policy & Procedure	Data Protection Procedure and Code of Practice
Policy Area	Human Resources
Version Number	03
Approving Committee	SMT
Date of Approval	08 May 2018
Date of Equality Impact Assessment	18 May 2018
Date of Review	08 May 2021
Responsible Senior Manager	Director Organisational Development & HR

History of Amendments

Date	Version/Pages/Sections Affected	Summary of changes
09 June 2015		
April 2017	Pages 19/20	Retention details updated
April 2018	Whole document	Revised for implementation of GDPR

Policy Statement

The General Data Protection Regulation (GDPR) requires the College to process any personal data in accordance with the GDPR Data Protection Principles and ensure that we meet our legal obligations as laid down in Data Protection Law (including the GDPR and all relevant EU and UK data protection legislation).This Procedure has been introduced to enable the College to comply with the requirements of the GDPR.

Equality Statement

The College is committed to providing equal opportunities to ensure its students, staff, customers and visitors are treated equally regardless of gender reassignment, race, religion or belief; disability; age; marriage and civil partnerships; pregnancy and maternity; sexual orientation; sex.

Please note this document is available in other formats, to request another format please email info@wcs.ac.uk

Contents

Data Protection Procedure and Code of Practice

1. Introduction

Data Protection Law regulate the processing of information relating to living individuals ("personal data"), including the obtaining, holding, use or disclosure of such personal data.

West College Scotland ("the College") holds a wide range of personal data about individuals such as its employees, students, former students and others (who are defined as "data subjects" in the General Data Protection Regulation (GDPR) to allow it to carry out many of its functions, for example, organising and operating courses, complying with legal obligations, e.g. health and safety and recruiting, managing and paying staff.

This procedure applies to all processing of personal data for the College's purposes, by staff, students and others.

The College, as data controller, remains responsible for the control of personal data it collects even if that data is later passed onto another organisation or is stored on systems or devices owned by other organisations or individuals (including devices personally owned by members of staff). Personal data must be processed in accordance with the Data Protection Law and, in particular, the Principles relating to the processing of personal data set out in Article 5 of the GDPR.

2. Status of this Procedure

This procedure is not contractual and will be subject to amendment by the College from time to time. Staff and students are expected to abide by the procedure that is in place at any particular time. Any failure to follow the procedure may result in disciplinary proceedings.

3. Definitions

3.1. "Controller" is defined by the GDPR as the natural or legal person, public authority, agency or other body which, alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller of the specific criteria for its nomination may be provided for by Union or Member State law.

3.2. "Processor" is defined by the GDPR as a natural or legal person, public authority,

agency or other body, which processes personal data on behalf of the controller

3.3. "Data subject" is defined by the GDPR as an identified or identifiable natural person

3.4. "Personal data" is defined by the GDPR as any information relating to an identified natural person (data subject); an identifiable natural 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 natural person. It refers to information processed wholly or partly by automated means and to processing other than by automated means of data which forms part of a filing system or which is intended to form part of a filing system.

3.5. "Filing system" is defined by the GDPR as any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographic basis.

3.6. "Special Categories of personal data" are defined by the GDPR as personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. Data relating to criminal convictions and offences will also be treated as special category data under this policy.

3.7. "Processing" is defined by the GDPR as 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.

4. Principles

The principles relating to the processing of personal data require that personal data shall be:

a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible

with the initial purposes ('purpose limitation');

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

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');

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

The Data Controller shall be responsible for, and be able to demonstrate compliance with Principles.

5. The Data Controller

The College is the Data Controller under the GDPR.

6. Data Protection Officer

The College's Data Protection Lead is the Director Organisational Development and HR. The College Data Protection Officer is Donald MacLean and he can be contacted at donald.macLean@wcs.ac.uk

Any questions or concerns about the interpretation or operation of this procedure should be taken up with the Data Protection Officer.

7. Responsibilities of Staff, Students and others who provide personal data to the College

All staff, students and others who provide personal data to the College are responsible for ensuring that the personal data they provide to the College is accurate at the time it is given and for informing the College of any changes to the personal data that they have provided to it, e.g. change of address. The College cannot be held responsible for any errors in the personal data it holds unless the staff member, student or other individual informs the College of such changes.

8. Staff and others who process personal data in respect of which the College Is the Data Controller

All staff and others who process personal data in respect of which the College is the Data Controller, are responsible for ensuring that they process personal data in accordance with this policy and Data Protection Law.

9. Students who process personal data in respect of which the College is the Data Controller

Students who process personal data in the course of their studies in respect of which the College is the Data Controller, must only process that personal data in accordance with the instructions given to them by their tutor, Lecturer or member of Support staff. Students who process personal data in respect of which the College is the Data Controller, must ensure that they process personal data in accordance with this policy and Data Protection Law.

10. Data Security

All staff and students are responsible for ensuring that:

- any personal data that they hold is kept securely; and
- personal data is not disclosed orally, in writing or via web pages or by any other means, intentionally or otherwise, to any unauthorised third party.

Further guidance on how to keep personal data securely is found in the College's Data Protection Code of Practice. In particular:

- filed personal data must be kept in a locked cabinet, drawer, or safe
- where personal data is held on computer, access to the computer must be via a secured login using a complex password that is reset at regular intervals.

In addition, where personal data is held on a laptop computer, the laptop itself must be kept physically secure while in transit or while not in use.

Computerised personal data should be backed-up regularly.

Wherever possible, taking personal data off-site should be avoided. In particular, sensitive personal data should never be removed to an off-site location unless this is absolutely necessary and there is no other alternative.

Unauthorised disclosure of personal data is a disciplinary matter and may be considered gross misconduct in some cases.

11. Data Subject Rights

The GDPR provides data subjects with certain rights in respect of their personal data. These are:-

Subject access: the right to request information about how personal data is being processed including whether personal data is being processed and the right to be allowed access to that data and to be provided with a copy of that data along with the right to obtain the following information:

- the purpose of the processing;
- the categories of personal data;
- the recipients to whom data has been disclosed or which will be disclosed;
- the retention period;
- the right to lodge a complaint with the ICO;
- the source of the information if not collected direct from the subject; and
- the existence of any automated decision making.

Rectification: the right to allow you to rectify inaccurate personal data concerning you without undue delay.

Erasure: the right to have data erased in certain circumstances, and to have confirmation of erasure, but only where:

- the data is no longer necessary in relation to the purpose for which it was collected;
- where consent is withdrawn;
- where there is no legal basis for the processing; or
- there is a legal obligation to delete data.

Restriction of processing: the right to ask for certain processing to be restricted in the following circumstances:

- if you contest the accuracy of your personal data;
- if our processing is unlawful and you do not want it to be erased;
- if we no longer need the data for the purpose of the processing but it is required by you for the establishment, exercise or defence of legal claims; or
- if you have objected to the processing, pending verification of that objection.

Data portability: you have the right to receive a copy of the personal data you have provided to us and certain information generated by us, if our processing is carried by automated means, which will allow you to transfer it to another data controller. This only applies in relation to the data being processed by consent or under a contract to provide you with a service.

Object to processing: you have an absolute right to object to any direct marketing that we are sending to you and there are no exemptions to this which would allow you to refuse to comply.

Should you wish to exercise any of the rights noted above, please contact the Data Protection Officer

12. Rights to Access Personal Data

Staff must notify the Data Protection Officer of any request to exercise a data subject right as soon as it is received. All such requests must be responded to by the College within the timescale set down in the GDPR (currently one month).

In relation to Subject Access Requests, ideally the relevant Form should be completed. The College cannot insist upon this under Data Protection Law, but it will assist in the identification and locating of personal data and should be used where the data subject agrees.

The College will, upon receiving a valid subject access request, provide a data subject

with access to their personal data, subject to the application of relevant exemptions in Data Protection Law and the protection of the rights of other data subjects.

Notwithstanding the provisions of Data Protection Law, the College has resolved that a member of staff may inspect their personal file under supervision in the HR Department if they make a prior request in writing to the Director Organisational Development and HR giving 2 working days' notice. No copies of any documentation may be taken. This does not affect the rights of staff under Data Protection Law to make a subject access request.

13. External and Internal Assessment Evidence

The College will routinely provide students with information about the outcomes of their internal assessments, incorporating written feedback and marks allocated on coursework, projects and submitted work. Any written feedback and comments may well fall within the definition of personal data, and are not exempt from subject access provisions.

External Examination scripts, administered by the College and returned to awarding bodies, are exempt from the subject access provisions in Data Protection Law and will not ordinarily be provided to a student who requests them. Any queries about this should be made directly to the awarding body, for example, to SQA, who are the data controller.

14. Data Transfer

Where personal data is transferred internally, the recipient must only process the personal data in a manner consistent with the College's notification with the UK Information Commissioner's Office and within the original purpose for which the personal data was collected.

Personal data is not to be published on the internet or made available in any other form without the express permission of the Data Protection Officer.

15. Processing Special Categories of Personal Data

From time to time it is necessary for the College to process personal data which relates to an individual's health, criminal convictions, race, or trade union membership etc, which constitutes Special Category Data under the GDPR. More information about this is available from the Privacy Notice issued to all data subjects.

Sensitive categories of personal data will be processed in line with the privacy notice issued to all data subjects and will be retained in line with the Data Protection Code of Data Protection.

16. Publication of Personal Data

The names of senior managers and members of the Board of Management of the College will be published in the Annual Accounts and on the public website where there is any legal requirement to make such personal data public.

Certain personal data relating to College staff will be made available via searchable directories on the public website for the performance of that member of staff's duties in terms of their contract of employment and in order to meet the legitimate needs of visitors and enquirers seeking to make contact with appropriate staff. The College will make available the minimum personal data that is necessary to meet those legitimate interests. More information can be found in the College's Data Protection Code of Practice.

17. Retention of Personal Data

The College has a duty to retain some staff and student personal data for a period of time following their departure from the College, mainly for legal reasons, but also for other purposes such as being able to provide references and academic transcripts, or for financial reasons, for example, relating to pensions and taxation. Different categories of personal data will be retained for different periods of time. Information about the retention periods and purposes are set out in the Data Protection Code of Practice.

At the end of the relevant retention period, the College will securely erase or destroy the personal data.

18 Data Protection and References

Confidential references that are provided by the College are exempt from the subject access provisions of Data Protection Law in relation to any request made to the College. However, references that are received by the College from another person are not exempt. If the College receives a request for a reference received by it, the College will have regard to the rights under Data Protection Law of the provider of the reference.

19. Data Protection Code of Practice

1. Introduction

This Code of Practice must be read in conjunction with the College's Data Protection Policy document to give the fullest picture of West College Scotland's data protection regime. This document gives an introduction to some basic points of practice relating to the handling and processing of personal data at West College Scotland. It also lists the particular activities carried out within the College's support and academic departments that involve the processing of personal data. The College uses CCTV for a number of purposes. For further information and guidance on the college's processing of CCTV footage containing personal data, and for details of such processing, please see the College's CCTV Code of Practice available on the College intranet.

2. Key Concepts

The GDPR and the Data Protection Act 2018 places obligations upon West College Scotland, as a data controller, to collect and use personal data in a responsible and accountable fashion.

West College Scotland is committed to ensuring that every current employee and registered student complies with Data Protection Law to ensure the confidentiality of any personal data held by the College in whatever medium. Key concepts to be considered are those of purpose, fairness, lawfulness, transparency and security, which are all addressed in this Code of Practice.

3. Purpose

The Data Controller can only process personal data where they have a legal basis for doing so. The Code of Practice summarise the purposes for which the College processes personal data.

The College will:-

- only collect and process the personal data that is necessary for the purpose or purposes that we have identified in advance
- ensure that the legal basis for processing your data is identified in advance.
- ensure that as far as possible the personal data we hold is accurate
- only process your data for as long as is it required for our purposes and then we will securely dispose of, or delete your data
- provide data subjects with information on why we are asking for that data and what we intend to do with it
- not do anything with your data that you would not expect given the content of this policy and the fair processing or privacy notice.
- ensure that appropriate technical and organisational measures are in place to ensure the security of your personal data.

4. Fairness and Lawfulness

West College Scotland must process personal data fairly and lawfully and in accordance with the processing principles set out in the GDPR West College Scotland may also take advice from the Information Commissioner, the College's own legal advisors, and on wider practice within the UK FE / HE sector, as appropriate.

5. Transparency

Members of staff, students and others must be able to feel that there is no intention to hide from them details of how their personal data are collected, used and distributed by the College. One of the functions of this Code of Practice is to provide that assurance.

6. Existing Notifications

West College Scotland is a data controller registered with the Information Commissioner's Office (Registration Number ZA004894). The Students' Association is also registered as a Data Controller (Registration Number 00043242059). These entries can be examined on-line at the following Web address: https://ico.org.uk/about-the-ico/what-we-do/register-of-data-controllers/

It is very important that those who work with personal data in the course of their College duties are familiar with the details contained in these notifications.

6.1. Any changes that may be required should be passed to the Data Protection Officer as these entries are periodically reviewed and amended as necessary by the Data

Protection Officer.

6.2. Paragraph 6 of the Data Protection Policy gives details of the College's Data Protection Officer, who is responsible for handling subject access requests and dealing with data protection enquiries within the College.

7. Collection of personal data

In most cases, the personal data held by the College will be obtained directly from the data subjects themselves. The GDPR stipulates that the College must provide certain information to data subjects when their personal data is collected. Any members of staff responsible for managing the collection of personal data for the College must ensure that a notice containing the following information is included in the request for that data:

- A statement that West College Scotland is the data controller and our contact details
- The contact details of our Data Protection Officer
- A clear explanation of the legal basis for processing and the purposes for which that data will be processed
- The recipient or categories of recipients of the data
- Information about transfers to third countries including information about any relevant adequacy agreement or other safeguard in place and the means by which to obtain a copy of them or where they have been made available.
- The period for which the data will be stored/criteria used to determine that
- The right to request: access to; rectification of; erasure of; restriction of processing; or to object to processing; and the right of data portability
- The right to withdraw consent to processing
- The right to lodge a complaint with the ICO
- Where the processing is based on a statutory or contractual requirement, the consequences of failing to provide such data for the data subject should be given
- The existence of any automated decision making/profiling etc; how it works and the consequences of this processing for the data subject

8. Amendment of personal data

From time to time data subjects will wish to update some of their personal data held by the College, for example their home addresses or other contact details previously

submitted. To do this, the data subjects must either contact the specific member of staff designated in the data protection notice at the time the data was submitted, or the Data Protection Officer as set out in paragraph 6 of the Data Protection Policy. Proof of identity will be required before any amendments can be made.

8.1. With regard to 'self-service' computer-based support systems staff, students or others, the data subjects themselves will be responsible for the maintenance of certain elements of their personal records.

8.2. These systems will incorporate the necessary authentication and security mechanisms to ensure that data subjects are only able to view and amend their own data.

9. Security of Personal Data

Of fundamental importance within any data protection regime is the security of the personal data that is being processed. Data subjects have the right to expect that their personal data will be kept and processed securely and that no unauthorised disclosures or transfers will take place to anyone either within or outside the College. Authorised disclosures or transfers are those that are defined within the appropriate Notifications (see paragraphs 6–9 above) and declared to the data subject either at the point of data collection or subsequently, the necessary consent for disclosure or transfer having been obtained if required.

9.1. To help ensure the security of personal data within the College, all those in West College Scotland who process personal data in the course of performing their duties, are required to follow the general guidelines set out below.

10. Secure Processing of Personal Data

Each member of staff who, in the course of performing their legitimate duties, processes personal data, whether in electronic or paper format, must take reasonable precautions to ensure the safety and privacy of that data, in line with the Data Protection Procedure. For example:

- Filed personal data must be kept in a locked cabinet, drawer, or safe
- Where personal data is held on computer, access to the computer must be via a secured login using a complex password that is reset at regular intervals
- Where personal data is held on a laptop computer, the laptop itself must be kept physically secure while in transit or while not in use. There are many ways to secure this type of device e.g. propriety security cable, locked filing cabinet, drawer, or safe.

Individual circumstance will dictate

- It is important that a regular and secure backup schedule is applied to personal data
- If personal data is transferred to any type of removable storage media, that media must itself be kept secure while not in use. The copy of the personal data must be permanently deleted from the storage media as soon as it is no longer needed
- In open-plan offices, computer screens that could potentially be displaying personal data should not be positioned such that unauthorised staff may readily see that data
- Screen 'locking' should be invoked when a user with access to any type of personal data leaves the desk \ computer unattended for a short period. Log off and shut down are appropriate for longer periods away from the computer
- Personal data in manual form, such as in paper files, correspondence or database printouts, should not be left in view in open-plan offices while the relevant staff members are away from their desks. They should instead be locked away or securely stored
- Where manual records containing personal data are accessible to a number of staff in the course of their legitimate activities, access logbooks should be used where practicable to help monitor the whereabouts and use of such records.

11. Storage of Personal Data

11.1. Ordinarily, personal data should never be stored:

- at staff members' homes, whether in manual or electronic form
- at remote sites.

11.2. In cases where off-site processing is felt to be necessary or appropriate, the agreement of the relevant member of the Senior Management Team must be obtained, and all the security guidelines given in this document must still be followed.

11.3. Staff should be aware that log files will record details of all users who access, alter or delete or attempt to access, alter or delete centrally held computerised databases and files containing personal data.

12. The disclosure and transfer of personal data – Authorised and unauthorised disclosures

12.1. Staff members who process personal data on behalf of the College will be made aware by their line managers or other appropriate staff of the purposes for which the data is processed and the legitimate parties either within or outside West

College Scotland to whom that data, either in whole or in part, may be disclosed or transferred. Staff should also familiarise themselves with the College's Data Protection Register entry (see paragraphs 6-9 above) which includes details of the purposes for which personal data is processed, and the recipients to whom the College may disclose certain classes of personal data. Any queries about whether personal data can be processed in a particular way should be addressed to your line manager or the Data Protection Officer.

12.2. Personal information must not be disclosed either orally or in writing or via Web pages or by any other means, manual or electronic, accidentally or otherwise, to any unauthorised third party.

12.3. Staff should note that unauthorised disclosure will usually be a disciplinary matter, and may be considered gross misconduct in some cases.

13. Security of data during transfer

Where personal data is transferred between staff members within the College in the course of their legitimate activities, the level of security appropriate to the type of data and anticipated risks should be applied. For example, sensitive personal data should either be transferred by internal mail in sealed envelopes or by hand, if it cannot be securely transferred electronically. If transferred by e- mail, it should be sent in a password-protected attachment, with the password being supplied separately. Further advice on password protecting documents can be obtained from IT Department.

14. Disclosures outside the College

14.1. When a request to disclose or amend personal data held by the College is received from an individual or organisation outside the College, in general no data should be disclosed or amended unless the authority and authenticity of the request can be established. A Subject Access Request may be made by a third party on behalf of the data subject with the data subject's consent. Any such requests (e.g. from those claiming to be relatives or friends of the data subject) should be refused unless the consent of the data subject is obtained for such disclosures or where the College is satisfied that the person requesting the information has authority to do so. Such requests should be forwarded to the Data Protection Officer to respond to.

14.2. Requests for the disclosure of personal data from the Police, Government Bodies, the British Council or other official bodies and agencies should be investigated

sufficiently to verify the authenticity of the request and then should be passed to the Data Protection Officer to respond to. If there is a court order then the College is legally required to provide the personal data. If the request is made under the Data Protection Act 2018 then the College will only provide the information if satisfied that it can do so and comply with the law.

14.3. Details of any specific procedures and practices to be adopted when responding to requests for disclosure in individual departments within the College will be available from the appropriate senior members of staff.

14.4. The College will not transfer any personal data to a country outside the EU or an international organisation without appropriate safeguards being in place.

15. Publication of College Information

While the majority of personal data held by the College is processed for internal support purposes and is never disclosed outside the institution, some categories of personal data are routinely or from time to time released through one or more forms of publication. This personal data could be published on the public Web site or in college publicity materials such as the annual prospectus. Noted below in paragraphs 17 to 19 are the anticipated areas where such data may be published.

16. Legal Obligations

When required by law the names of Senior Managers and members of the Board of Management of the College and certain other personal data relating to employees and members of the Board of Management are published on the Web site. The College also fulfils all obligations placed upon it by its relationship with various funding bodies, Government Agencies and the like with regard to the release of personal data and statistical information concerning students and staff. Data subjects are informed of the College's obligations in this respect at the time the data is collected.

17. Staff Directory

For the performance of staff duties in terms of the terms of their contract of employment and in order to meet the legitimate needs of visitors and enquirers to be able to make contact with appropriate staff, the College may at some future date make available on its public Web site a directory containing the job title, organisational unit, title, forename, surname, office telephone number, office room number and location and office e-mail address of each staff member. A complete directory is currently available on the College intranet and is only available to current staff. At the time of

appointment or at the point the personal data is made available via the directory for the first time, each individual member of staff will be advised of the data which will be made available. At any time (via a request to the Data Protection Officer) each individual member of staff will be able to request that their personal data, or any part of their personal data will not appear in this public directory. The Web- based public directory will be searchable by name and organisational unit and will only return personal data for those staff who have not asked for it to be removed.

18. Staff personal data on Web pages

Apart from the staff directory described above, staff biographical details or other personal data may be published on West College Scotland's Web sites or in other media. However, publication in this way does not mean that such data can be reproduced without permission. West College Scotland retains control and copyright of such data and the data must not be reproduced or further processed without the College's express permission.

19. Student personal data on Web pages

Apart from the obligations mentioned above (paragraph 18) the College will not ordinarily reveal any personal data of students enrolled at West College Scotland to any individual or body outside the College. It may also be the case that students enrolled on certain courses may produce Web-based material containing personal data as part of their course work. In such cases, responsibility for such disclosures rests entirely with the individual students concerned and is not indicative of any College-wide policy. Where a student is concerned with the release of personal data they should either contact their tutor for advice or contact the Data Protection Officer

20. Retention and Disposal of Personal Data

20.1. The retention of personal data

The College has a duty to retain some staff and student personal data for a period of time following their departure from the College, mainly for the purposes of being able to provide references and academic transcripts, or for financial reasons, for example relating to pensions and taxation. Some material will also be retained to form part of the official College archive. The retention periods selected follow the guidance given in the JISC publication 'Study of the Records Life Cycle', Different categories of data will be retained for different periods of time, and these are set out in the following table.

20.2. The disposal of personal data

When a record containing personal data is to be disposed of, the following procedures will be followed:

- All paper or microfilm documentation containing personal data will be permanently destroyed by shredding or incinerating, depending on the sensitivity of the personal data.
- All computer equipment or media that are to be sold or scrapped will have had all personal data completely destroyed, by re-formatting, over-writing or degaussing.

20.3. Employees and, where appropriate, students, will be provided with guidance as to the correct mechanisms for disposal of different types of personal data and audits will be carried out to ensure that this guidance is adhered to. In particular, employees and students will be made aware that erasing/deleting electronic files does not equate to destroying them.

Type of Record	**Minimum Retention Period**	**Reason for Length of Period**
Personnel files including training records, notes of disciplinary and grievance hearings, and appraisal forms	6 years from the end of employment	References and potential litigation (Prescription and Limitation (Scotland) Act 1973) Selected material will form part of the official College Archive
Letters of reference	6 years from the end of employment, by the author of the reference letter	References and potential litigation (Prescription and Limitation (Scotland) Act 1973)
Application forms/interview notes	At least 6 months from the date of the interviews	Time limits on litigation (Equality Act 2010)
Facts relating to redundancies where	6 years from the date of redundancy	Potential litigation, (Prescription and

Type of Record	Minimum Retention Period	Reason for Length of Period
fewer than 20 redundancies		Limitation (Scotland) Act 1973)
Facts relating to redundancies where 20 or more redundancies	12 years from the date of the redundancies	Potential litigation, (Prescription and Limitation (Scotland) Act 1973) & having a business record of facts relating to collective redundancies.
Income Tax and NI Returns, including correspondence with tax office	At least 3 years after the end of the financial year to which the records related	Income Tax Pay As You Earn Regulations 2003
Statutory Maternity Pay records and calculations	As above	Statutory Maternity Pay (General) Regulations 1986
Statutory Sick Pay records and calculations	As above	Statutory Sick Pay (General) Regulations 1982
Wages and salary records	6 years after financial year to which relate	Taxes Management Act 1970
Accident books, and records and reports of accidents	3 years after the date of the last entry	Social Security (Claims and Payments) Regulations 1979; RIDDOR 2013
Health Records relating to Health Surveillance	40 years	Management of Health and Safety at Work Regulations

Type of Record	**Minimum Retention Period**	**Reason for Length of Period**
Health Records where reason for termination of employment is connected with health, including stress related illness	3 years	Limitation period for personal injury claims (Prescription and Limitation (Scotland) Act 1973)
Medical records kept by reason of the Control of Substances Hazardous to Health Regulations 2002	40 years	The Control of Substances Hazardous to Health Regulations 2002
Applicant records for those who are rejected or who decline an offer	6 months after the start of the academic year	Permits institution to handle enquiries from the data subject and reflects time limits in Equality Act 2010
Student records of those not completing enrolment	Within one academic year	Permits institution to handle delayed enrolments
Student records, including enquiries, applications, admissions, assessment, awards, attendance and conduct	At least 6 years from the date that the student leaves the institution, in case of litigation for negligence At least 10 years for personal and academic references	Limitation period for litigation (Prescription and Limitation (Scotland) Act 1973) Permits institution to provide references for a reasonable length of time

Type of Record	Minimum Retention Period	Reason for Length of Period
		While personal and academic references may become 'stale', some data e.g. transcripts of student marks may be required throughout the student's future career. Upon the death of the data subject, data relating to him/her ceases to be personal data. Some selected material will form part of the official College Archive.
Records documenting the formulation of plans for the implementation of the institution's finance strategy.	+ 10 years	So that the College has an accurate and detailed record of its finance strategy over time.
Records documenting the conduct and results of financial audits, and action taken to address issues raised.	Last action on audit + 6 years	Prescription and Limitation (Scotland) Act 1973
Records documenting all financial transactions.	Current financial year + 6 years	Prescription and Limitation (Scotland) Act 1973
Records documenting Invitations to Tender and tender evaluation criteria.	Termination of supply contract awarded + 6 years	Prescription and Limitation (Scotland) Act 1973

Type of Record	Minimum Retention Period	Reason for Length of Period
Records documenting the arrangement and renewal of insurance policies to meet defined requirements and legal obligations: employers' liability insurance.	Commencement of policy + 40 years or renewal of policy + 40 years	So that the College has an accurate and detailed record of its insurance cover over time

21. The Processing of Personal Data within Specific Departments – Activities involving the processing of personal data:

Activities carried out within the College that involve record processing are identified in the Data Register which is maintained by the Data Protection Officer. It is the responsibility of the appropriate Managers to ensure that sufficiently detailed guidance is given to their staff to enable them to carry out these activities in accordance with the requirements of the Act.

Annex 1

West College Scotland
Subject Access Request Form

1. Details of the person requesting the form and preferred method of contact	
Full Name:	
Address:	
Telephone Number:	
Email address:	
2. Are you the Data Subject?	
Yes:	
If you are the Data Subject please supply evidence of your identity i.e. passport, driving licence, birth certificate (or photocopy). We recommend if sending originals by post you use recorded delivery. We will return any originals you send us by recorded delivery, or you can arrange to collect in person. Please also state your relationship to West College Scotland:	
I am a current / former member of staff	
I am a current / former student	
I am neither of the above	
Please now go to question 5	
No:	
Are you acting on behalf of the Data Subject with their written authority? If so, that authority must be enclosed. Please also state the relationship of the Data Subject to West College Scotland:	
The Data Subject is a current/former member of staff	
The Data Subject is a current/former student	
The Data Subject is neither of the above	
Please now go to questions 3 and 4.	
3. Details of the Data Subject (if different from 1.)	
Full Name:	
Address:	
Telephone Number:	
Email address:	

4. Please describe your relationship with the Data Subject that leads you to make this request for information on their behalf.	
5. If you wish to see only certain specific personal data, for example that contained in a particular examination report, a specific departmental file etc, please describe these below:	
6. If you would like a more general search, please note that the College is able to search the following sections for personal data. Please indicate the sections that you would like searched:	
Student Records	
Human Resources	
Library	
Finance	
Teaching section files and information systems	
Please specify which Faculty: Other Support Department Files and Information Systems	
Please specify which Support Section (s):	
7. Declaration: I certify that the information given on this application form is true. I understand that it is necessary for the College to confirm my/the Data Subject's identity and it may be necessary for more detailed information to be obtained in order to locate the correct information.	
Signed:	
Date:	

Please return the completed form to the Data Protection Officer at the address given below:
West College Scotland, Queens' Quay, Clydebank, G81 1BF or email dpo@wcs.ac.uk
Documents which must accompany this application are: • evidence of your identity • evidence of the Data Subject's identity (if different from above) • evidence of the Data Subject's consent to disclose to a third party (if required as indicated above) Please note that in responding to your request the College may withhold personal data under the terms of Data Protection Law.

Office Use Only	
Request received:	
Date completed:	
Notes:	

EQUALITY IMPACT ASSESSMENT

Name of Procedure:	Data Protection Procedure and Code of Practice.

Responsible Person:	Clare Fraser	**Date:**	18 May 2018

Provide a brief summary of the aims of the policy/procedure/decision and main activities:
This Procedure and Code sets out the procedure for the processing of personal data by West College Scotland. It has been developed to ensure that College processes comply with the General Data Protected Regulation.

This stage establishes whether a policy, procedure or decision will have a differential impact from an equality perspective on people who share protected characteristics or whether it is "equality neutral" (i.e. have no effect either positive or negative).

The protected characteristics are: age, disability, gender reassignment, pregnancy or maternity, race, religion or belief, sex and sexual orientation.

1. Who will benefit from this (students/staff/stakeholders)? Is there likely to be a positive impact on people who share protected characteristics, and if so, how? Or is it clear at this stage that it will be equality "neutral"? i.e. will not have a differential impact on any equality group/s?

This Procedure should benefit all staff and students as it should increase confidence in how WCS processes personal data. There will be particular benefits for people who share the protected characteristics of race, disability, sex, sexual orientation and religion or belief as information relating to these characteristics is defined by the GDPR as "special categories of personal data". Accordingly, there are additional measures in place to ensure that such information is processed sensitively and confidentially.

2. Is there likely to be an adverse impact on people who share protected characteristics? If so, who may be affected and why? Or is it clear at this stage that it will be equality "neutral"?

This policy has been developed to comply with UK law and will not have an adverse impact on people who share protected characteristics.

3. What action will you take to ensure that you are monitoring the impact of this policy?

Monitoring of this policy will take place through Complaints and HR grievances data.