ST MARY'S UNIVERSITY COLLEGE

DATA PROTECTION POLICY

1. Introduction

1.1 St Mary's University College is required by law to comply with the General Data Protection Regulation (GDPR) and Data Protection Act 2018. This policy sets out how the College will protect the rights and privacy of individuals in accordance with the Act.

2. Purpose and Scope

2.1 College staff and students, or others who process or use any personal information on behalf of the College (i.e. "data users"), have a personal responsibility to ensure that they adhere to the College's Data Protection Policy, GDPR and the Act.

2.2 In carrying out its responsibilities, the College will be required to process certain information about individuals such as staff, students, graduates and other users, defined as "data subjects" in the Act. This information, or "data" as it is often referred to, must be processed according to the Data Protection Principles contained within the Act.

2.3 Any breaches of this Policy or the GDPR, by a member of staff or student can be considered a disciplinary matter. It may also be a criminal matter for which the College and the individual concerned could be held criminally liable.

2.4 The GDPR defines both personal data and special category personal data (please refer to Appendix 1 Definitions). Data users must ensure that the necessary conditions are satisfied for the processing of personal data. In addition, they must adhere to the extra, more stringent conditions in place for the processing of special category data.

2.5 Special Category Personal Data should only be processed if it meets one of the conditions for processing detailed in Appendix 2 of this policy. It is recommended that special category records are kept separately in a locked drawer or filing cabinet or in a password-protected computer file.

2.6 The Board of Governors holds ultimate responsibility for approving this Data Protection Policy, overseeing its implementation, and ensuring ongoing compliance with the General Data Protection Regulation (GDPR) and Data Protection Act 2018. The Board will regularly review data protection practices, monitor compliance, and receive assurance reports to confirm adherence to statutory obligations and best practice standards

3. Data Protection Principles

3.1 The College is committed to ensuring that all employees, registered students, agents, contractors and data processors comply with the Act, regarding the processing and confidentiality of any personal data held. In order to do this St Mary's University College must comply with the six Data Protection Principles.

3.2 Personal data must be:

- Processed, lawfully, fairly and in a transparent manner.
- Collected for specified, explicit and legitimate purposes.
- Adequate, relevant and limited to what is necessary.
- Accurate and where necessary up to date.
- Kept in a form which permits identification of data subjects for no longer that is necessary for which those data are processed; and
- Processed in a manner that ensures appropriate security of the personal data.

3.3 Accountability is central to the GDPR. As a data controller, St Marys University is responsible for compliance with the principles and must be able to demonstrate this to data subjects and the regulator (the Information Commissioner).

4. Lawfulness of processing

4.1 The College will identify the lawful basis for processing personal data.

4.2 The lawful basis for processing is set out in Article 6, GDPR and at least one of these conditions must apply whenever the College processes personal data.

Consent	The individual has given clear consent to process their personal data for specific purpose
Contract	The processing is necessary for a contract which you have with the individual or because they have asked you to take specific steps before entering into a contract
Legal Obligation	The processing is necessary for the College to comply with the law (not including contractual obligations)
Vital Interests	The processing is necessary to protect someone's life.
Public Task	The processing is necessary to perform a task in the public interest or official functions and the task or functions has a clear basis in law.
Legitimate Interests	The processing is necessary for your legitimate interests of the legitimate interests of a third party, unless there is good reason to protect the individual's personal data which overrides those legitimate interests. (This does not apply where the College is processing data to perform official tasks).

The College will provide information to data subjects about the lawful basis for processing within a privacy notice.

5. Rights of data subjects

5.1 Data subjects are afforded a number of rights under the GDPR. The are:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automate decision making and profiling.

5.2 The right to be informed

The College will inform data subject through a privacy notice, how personal data held by the College, whether obtained directly or not is processed.

The information the College will supply about the processing of personal data must be

- Concise, transparent, intelligible and easily accessible
- Written in clear and plan language, particularly if addressed to a minor
- Free of charge

5.3 The rights of access

Under GDPR, data subjects will have the right to obtain

- Confirmation that their data is being processed
- Access to their personal data
- Other supplementary information (this corresponds with the information provided in the privacy notice).

The college will provide a copy of the information free of charge. A "reasonable fee" may be required, or a request may be refused where it is manifestly unfounded or excessive, particularly if repetitive.

If the request is refused an explanation as to why will be provided and the data subject will be informed of their right to complain to the Information Commissioner.

The Identity of a data subject may be verified before release through the provision of relevant identification documents.

Where possible and proportionate, the College will provide the data requested in the preferred format of the applicant.

Whilst data subjects have the general right of access to their own personal information, which is held, the College will be mindful of those circumstances where an exemption may apply and in particular the data protection rights of third parties who may also be identifiable form the data being requested.

5.4 The right to rectification

The College will rectify personal data where it is inaccurate or incomplete.

Where the College has disclosed the personal data in question to others, each recipient will be contacted and informed of rectification unless this is impossible or involves disproportionate effort.

A request for rectification can be made via email to admissions@smucb.ac.uk and will be responded to within one month. Where a request is particularly complex the College may request an extension, up to an additional two months

Where the College cannot take action to rectify an explanation will be provided to the data subject and they will be informed of their right to complain to the Information Commissioner and to judicial remedy.

5.5 The right to erasure – also known as "the right to be forgotten"

Where there is no compelling reasons for the continued processing of an individual's personal data the College will delete or remove the personal data at the request of the data subject.

Data may be erased to prevent processing in the following circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed:
- When the individual withdraws consent
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing
- The personal data was unlawfully processed (i.e. otherwise in breach of the GDPR).
- The personal data has to be erased in order to comply with a legal obligation
- The personal data is processed in relation to the offer of information society services to a child.

(Under the GDPR, this right is not limited to processing that causes unwarranted and substantial damage or distress. However, if the processing does cause damage or distress, this is likely to make the case for erasure stronger).

A request for erasure may be refused where the personal data is processed for the following reasons:

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

If the personal data in question has been disclosed to others, we will contact each recipient and inform them of the erasure of the personal data - unless this proves impossible or involves disproportionate effort. Upon request the College will inform the individual about these recipients.

5.6 Right to restrict processing

The College will restrict the processing of personal data in the following circumstances:

- Where an individual contests the accuracy of the personal data, we will restrict the processing until the accuracy of the personal data has been verified.
- Where an individual has objected to the processing (where it was necessary for the performance of a public interest task or purpose of legitimate interests), and you are considering whether your organisation's legitimate grounds override those of the individual.
  • When processing is unlawful and the individual opposes erasure and requests restriction instead.
- If we no longer need the personal data but the data subject requires the data to establish, exercise or defend a legal claim.

Where the personal data in question has been disclosed to others, we will contact each recipient and inform them of the restriction on the processing of the personal data - unless this proves impossible or involves disproportionate effort. If asked to, the College will also inform the data subject about these recipients. The College will inform the data subject if it is decided to lift a restriction on processing.

5.7 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 and allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.

The right to data portability only applies:

- to personal data an individual has provided to a controller
- 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.

Where the data requested meets these requirements the College will provide the personal data in a structured, commonly used and machine-readable form and free of charge. If the data subject requests it, the College will transmit the data directly to another organisation, if this is technically feasible. The College will respond without undue delay, and within one month. This can be extended by two months where the request is complex, or the College has received a large number of requests.

5.8 Right to object

Individuals have the right to object to:

- Processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling);
- Direct marketing (including profiling); and
- Processing for purposes of scientific/historical research and statistics.

The College will stop processing the personal data unless:

- There are compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual; or
- The processing is for the establishment, exercise or defence of legal claims.

Where appropriate the College will inform individuals of their right to object "at the point of first communication" and Its privacy notice. This will be "explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information". The College will stop processing personal data for direct marketing purposes as soon as we receive an objection. Where the College is conducting research where the processing of personal data is necessary for the performance of a public interest task, it is not required to comply with an objection to the processing.

5.9 Rights related to automated decision-making including profiling

The College will carry out processing under Article 22(1) of the GDPR where the College is authorised or required to do so and it is the most appropriate way to achieve the aims of processing.

6. Security

6.1 The security of personal information in the possession of the College is of paramount importance and is therefore addressed in other policies and procedures. In addition to the principles and procedures contained within this section of the policy, staff/students are also advised to read and adhere to the College's IT Policies including Rules of Use and Security Policy.

7. Responsibilities - General Principles

7.1 All personal data held on behalf of the College, whether electronically or on paper must be kept securely, no matter whether it is kept by an individual or the College administration. Personal data must not be disclosed to any unauthorised third party by any means, accidentally or otherwise.

7.2 Staff are reminded that it is the individual's responsibility to adhere to this policy document. Where staff are unsure of the legal basis for sharing or disclosing information, either within or outside of the College, they must seek clarification from their line manager or the Data Protection Officer.

7.3 Any unauthorised disclosure or breach of the College's Data Protection Policy or the Act by a member of staff or student, can be considered as a disciplinary matter. It may also be a criminal matter for which the College and the individual concerned could be held criminally liable.

7.4 Department Responsibilities

The Data Protection Officer together with senior post holders within departments have responsibility for ensuring that:

- All staff are briefed on the Act, GDPR and the University College's Data Protection Policy (including any subsequent amendments or additions)
- All personal data being processed within the department complies with the GDPR, DPA 2018 and the University College's Data Protection Policy and is included in the University College's official Data Protection Notification.
- Mechanisms are implemented and routinely reviewed to protect data (particularly sensitive data) during day-to-day operations.
- An audit of the personal data within the department is carried out and recorded.
- That all forms and correspondence used by the department to request personal data, clearly state the purposes for which the information is to be used, the period of time it is to be retained, and to whom it is likely to be disclosed.
- All contractors, agents and other non-permanent University College staff used by the department, are aware of and comply with, the GDPR, DPA 2018 and the University College's Data Protection Policy.

- All personal data held within the department is kept securely and is disposed of in a safe and secure manner when no longer needed.
- All Data Protection breaches are notified to the Data Protection Officer using the appropriate form and in line with Data Breach procedures.
- Where a new or different purpose for processing data is introduced, the Data Protection Officer is informed. This will include the requirement to carry out an impact assessment for new information systems, which store or processes personal data.

7.5 Staff Responsibilities:

All staff must ensure that:

- They are aware of their responsibilities in this area, and the risks associated if failing to comply with the Data Protection Policy and the Act. Where they are uncertain of their responsibilities, they must refer this to their line manager.
- They complete the mandatory online training programme.
- Personal data which they provide in connection with their employment is accurate and up-to-date, and that they inform the University College of any errors, corrections or changes, for example, change of address, marital status, etc.
- Personal data relating to living individuals (staff, students, contractors, members of the public etc.) which they hold, or process is kept securely.
- Personal data relating to living individuals is not disclosed in any form to any unauthorised third party. Unauthorised disclosure may be considered a disciplinary matter.
- Any Data Protection breaches are notified to their line manager and Data Protection Officer and agreed remedial actions are implemented.
- When supervising students who are processing personal data, that those students are aware of the Data Protection Principles, and the University College's Data Protection Policy.

7.6 Student Responsibilities

All students must ensure that:

- Personal data which they provide in connection with their studies is accurate and up-to-date, and that they inform the College of any errors, corrections or changes, for example, change of address, marital status, etc.
- When using College facilities to process personal data (for example, in course work or research), they notify their staff supervisor / advisor in the relevant department, who will provide further information about the College's policy on data protection compliance.

The College shall not be held responsible for errors of which it has not been informed.

7.7 Data Protections Officer's Responsibilities

The Data Protection Officer must ensure that:

• The College's Data Protection Policy is regularly reviewed and updated in line with best practice.

• Staff have access to training on their responsibilities under the Policy, the GDPR and the Data Protection Act 2018, both on-line and through more traditional training methods.

• Responses to requests for information and related compliance matters are dealt with in a timely manner and in line with the requirements of data protection legislation.

• Advice on any area of the policy or data protection legislation is provided to staff and students, on request.

8. Notification

8.1 The College will register as a Data Controller and a Data Processor is required to provide the Information Commissioner detailing the following: -

- The personal data that it will process
- The categories of data subject to which personal data relates
- The purposes for which the personal data will be processed
- Those people to whom the College may wish to disclose the data
- Any countries or territories outside the European Economic Area to which the College may wish to transfer the personal data
- A general description of security measures taken to protect the data

8.2 When processing for a new or different purpose is introduced, the individuals affected by that change will be informed and the official notification will be amended.

8.3 Upon request the College shall notify all staff, students and other relevant data subjects of the types of personal data held by the College about them, and the reasons for which it is held/processed. The information currently held by the College and the purposes for which it is held/processed, form the official notification that has been submitted to the Information Commissioner's Office.

9. Disposal Policy for Personal Data

9.1 The GDPR places an obligation on the University to exercise care in the disposal of personal data, including protecting its security and confidentiality during storage, transportation, handling and destruction.

9.2 All staff have a responsibility to consider safety and security when disposing of personal data in the course of their work. Consideration should also be given to the nature of the personal data involved including how sensitive it is, and the format in which it is held. Details of the College's disposal policy can be found in Appendix 3.

10. Retention Policy for Personal Data Records

10.1 The GDPR places an obligation on the University not to hold personal data for longer than is necessary. Appendix 4 provides guidance as to the length of time that personal data should be retained by the College.

11. Contractors, Short-Term and Voluntary Staff

11.1 The College is responsible for the use made of personal data by anyone working on its behalf, whether as, an agent, or in a voluntary capacity, or as a consultant or contractor undertaking work for the College.

12. Transfer of Data Outside the College

Where the College shares personal data with another organisation, the College must ensure that the organisation has in place the requisite controls and security to demonstrate compliance with the GDPR.

If Staff must share personal data with other organisations in order to conduct business, a data sharing agreement may be required. Please contact the Colleges Data Protection Officer for guidance.

13. Transfer of Data Overseas

13.1 GDPR prohibits the transfer of personal data to any country outside the UK and European Economic Area (EEA) (EU Member States, Iceland, Liechtenstein and Norway,) unless that country ensures an adequate level of protection for data subjects.

13.2 In all instances where personal data is being sent outside the E.E.A. the consent of the data subject should be obtained before their personal information is sent. This includes requests for personal data from overseas colleges, financial sponsors, foreign governments etc.

14 Use of CCTV

14.1 The College's use of CCTV is governed by a Code of Practice, issued by the ICO:
Video surveillance (including guidance for organisations using CCTV) | ICO
For reasons of crime prevention and security, a network of surveillance cameras are in operation throughout campus. The presence of these cameras may not be obvious. This policy determines that personal data obtained during monitoring will be processed as follows:

- Any monitoring will be carried out by a limited number of specified staff
- The recordings will be accessed only by authorised personnel
- Personal data obtained during monitoring will be destroyed as soon as possible after any investigation is complete
- Staff involved in monitoring will maintain confidentiality in respect of personal data.

15. Making a Request

15.1 Staff, students, users of the College's facilities, and members of the public have the right to access personal data that is being kept about them insofar as it falls within the scope of the Act. Requests should be made in writing via email to m.mulholland@smucb.ac.uk or via post to:

The Data Protection Officer
Academic Registry
St Mary's University College
191 Falls Road
Belfast
BT12 6FE

Appendix 1

Definitions

Data	Information which is being used or held in a computerised system or a 'relevant filing system that is structured in such a way that data contained within is readily accessible. Data can be written information, photographs, fingerprints or voice recordings.
Personal Data	Information relating to natural (living) persons who can be identified or who are identifiable, directly from the information in question; or who can be indirectly identified from that information in combination with other information.
Special Category Data	Personal data consisting of information as to race/ethnic origin/ political opinion, religious or similar beliefs; trade union membership; physical or mental health or condition; sexual life; sexual orientation; genetics and biometrics (where used for ID purposes)
Criminal Offence Data	Personal data relating to criminal convictions and offences or related security measures.
Processing	Anything that can be done with personal data i.e. obtaining, recording, holding, organising, adapting, altering, retrieving, consulting, disclosing, aligning, combining, blocking, erasing, destroying etc.
Data Subject	An individual who is the subject of personal data. This will include staff, current and prospective students, graduates, suppliers of goods and services, business associates, conference delegates, survey respondents etc.

Data Controller	Refers to St Mary's University College Belfast. This includes college staff who collect and process data on behalf of the College, and students who are collecting and processing personal data or as part of their studies.
Data Processor	Any person (other than an employee of the College) who processes personal data on behalf of the College.
Data Users	Refers to both Data Controller and Data Processors.

Conditions for processing special category data

The conditions are listed in Article 9(2) of the GDPR:

1. The data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject.
2. The processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;
3. The processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent
4. The processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;
5. The processing relates to personal data which are manifestly made public by the data subject
6. The processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity
7. The processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject
8. The processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;
9. The processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

   Read these alongside the Data Protection Act 2018, which adds more specific conditions and safeguards.

DISPOSAL POLICY - REQUIRED PROCEDURES

1. Authorisation

The destruction of University College records must be authorised by senior post holders. If there is any doubt about the need for authorisation in a specific case, individuals should consult their line managers.

2. Safe and Secure Disposal

When records are disposed of, it is important to use methods that do not allow future use or reconstruction. Paper records containing personal data should be shredded and must not be simply thrown out with other rubbish or general records.

Special care must be taken with electronic records, which can be reconstructed from deleted information. Similarly, erasing or reformatting computer disks or personal computers with hard drives, which once contained personal data is not enough. Software tools are available which will remove all data from the medium so that it cannot be reconstructed.

Videotapes containing personal data should also be physically destroyed, not simply thrown away. Overwriting a videotape which contains personal data with non-personal information will remove the previous images; this should be done on-site by authorised staff.

3. Off-site Disposal

When records are destroyed by an outside agency, that agency should be contractually bound to observe the same security standards and considerations as those that apply to on-site disposal.

4. Disposal Record

A disposal record is a list indicating who has destroyed what records, when, and using what method of destruction. The disposal record applies to both paper and electronic (computer and video) records. It must not, in itself, contain personal data. Refer to the record type rather than the contents of the record. For example, "2007 PGCE Students " would be acceptable, " John Kearney, Ann McLaughlin, etc " would not.

Each department should create and maintain a disposal record for personal data.

APPENDIX 4

RETENTION POLICY FOR PERSONAL DATA RECORDS

Ref No.	Type of Record	Suggested Retention Period	Reason for Length of Period
1	Personnel files including training records and notes of disciplinary and grievance hearings	7 years from the end of employment	References and potential litigation.
2	Application forms/interview notes	At least 12 months from the date of the interviews	Time limits on litigation
3	Facts relating to redundancies where less than 20 redundancies	7 years from the date of redundancy	Time limits on litigation
4	Facts relating to redundancies where 20 or more redundancies	12 years from the date of the redundancies	Limitation Act 1980
5	Income Tax and NI Returns, including correspondence with tax office	7 years after the end of the financial year to which the records related	Income Tax (Employment) Regulations 1993
6	Statutory Maternity Pay records and calculations	At least 3 years after the end of the financial year to which the records related	Statutory Maternity Pay (General) Regulations 1986
7	Statutory Sick Pay records and calculations	At least 3 years after the end of the financial year to which the records related	Statutory Sick Pay (General) Regulations 1982
8	Wages and salary records	7 years	Taxes Management Act 1970

9	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 1985
10	Health Records	During employment	Management of Health and Safety at Work Regulations
11	Health Records where reason for termination of employment is connected with health, including stress related illness	3 years	Limitation period for personal injury claims
12	Medical records kept by reason of the Control of Substances Hazardous to Health Regulations 1999	40 years	Control of Substances Hazardous to Health Regulations 1999
13	Ionising Radiation Records	At least 50 years after last entry	Ionising Radiations Regulations 1985
14	Student records, including academic achievements and conduct Examination Scripts & Assessment Papers Student Fees, Loans and	At least 6 years from the date that the student leaves the institution, in case of litigation for negligence 1 year after graduation	Limitation period for negligence. In the event of an appeal from either the student or a legal source.

	Bursary Information	7 years	In accordance with Financial/ Audit and Accounting requirements.
	Personal and academic references including placement details.	At least 10 years Certain personal data may be held in perpetuity.	Permits institution to provide references for a reasonable length of time. 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.
15	Alumni Records	Certain personal data may be held in perpetuity	Permits institution to provide alumni services unless data subject opts out.
16	Criminal Record Checks/ Disclosure Information	6 months after offer has been made and condition of satisfactory record check met or decision made.	Access NI Security Policy

17	Library Records including Fees due	1 year after leaving/ graduation	
18	External Suppliers including individual creditors/debtors. Personal details relating to payments for one off services or expenses	7 years	In accordance with Financial/ Audit and Accounting requirements.
19	Admission Application details	3 years including equal opportunity monitoring	Reporting of recruitment activity and Annual Programme Review
20	Research Records including personal data collected in audio, visual recording formats and documentation.	Minimum of 5 years after the project has been completed.	

REFERENCES

References Given by the College

Confidential references given by members of the University College, are exempted from subject access requests where those references relate to:

- Education, training or employment of the data subject
- appointment of the data subject to any office
  provision by the data subject of any service.

The College has the absolute discretion to refuse to release confidential references written on their behalf if requested to do so in, or as part of, a subject access request.

References Received by The University College

Confidential references received by the College are not exempt from the right of access, but consideration must be given to the data privacy rights of the referee.

Information contained in, or relating to, a confidential reference can be withheld in response to a subject access request, if the release of this information would identify an individual referee unless:

- the identity of the referee can be protected by anonymising the information
- the referee has given their consent
- it is reasonable in all the circumstances to release the information without consent

In cases where a confidential reference discloses the identity of an organisation, but not an identifiable individual, as referee, disclosure will not breach data privacy rights, and the subject access request should be facilitated.

The College may not refuse to disclose references received in confidence from third parties without providing reasons.

References Internal to the College

Where an internal confidential reference is written and passed within the College about a data subject, it shall be subject to the same criteria as an external confidential reference received from a third party.

EXAMINATION SCRIPTS / MARKS

Examination scripts

Examination scripts are expressly exempted from the data subject access rules. This means that the College is under no obligation to permit examination candidates to have access to either original scripts or copies of the scripts.

Internal & External Examiners' Comments

Internal & External examiners' comments, whether made on the script or in another form that allows them to be held and applied to the original script (e.g. in a coded table), will be covered by the 2018 Act. A data subject has the right to request that a copy or summary "in intelligible form" is provided within the stipulated timescale, i.e. within 5 months from the date of the request, or 40 days from the announcement of the result, whichever is the earlier.

Examination Board Minutes and related documentation

Minutes of Examination Boards or Special Circumstance Committees that contain discussion about individuals will be open to data subject access, where candidates are named, or referred to by identifiers from which candidates may be identified (such as PINs), unless the data cannot be disclosed without additionally disclosing personal data about a third party.

Disclosure Of Results

As personal data, examination results should not be disclosed to third parties without the data subject's consent. Many institutions have traditionally publicly disclosed examination results in a variety of ways, including notice boards, newspapers, graduation documentation etc. Where such methods of publication continue to be used then disclosure should be confined to a traditional, local and limited nature. Students should be aware of where, and how, they may expect to see their results posted; and still retain the right to object to the use of their data in such a way.

ALUMNI

Alumni Records

Alumni are clearly a potentially valuable source of funding to any Higher Education Institution. An important first step is to be able to locate past students and correspond with them. When processing personal data the alumni office must adhere to the data protection principles and also take account of the fact that data subjects can request that their personal data are not processed for direct marketing purposes.

The alumni office should ensure that:

- Students are informed when their personal data is being collected that it will be used for alumni purposes and that the institution will wish to maintain contact with them after they finish their course of study.
- Students and alumni are able to opt out of the collection and processing of their personal data for such purposes.
- Students and alumni are able to request that where personal data is collected and processed for alumni contact purposes, the data is not used for direct marketing purposes.
- Students and alumni are provided with mechanisms whereby they can obtain the rectification, blocking, erasure, and destruction of their personal data, if necessary.

The mailing of University College magazines, and the solicitation of funds for charitable purposes may not constitute "direct marketing." However, if the College magazine contains advertising inserts, or if the mailing is about a University College credit card (an increasingly popular idea) these may be considered the direct marketing of products and services for which an opt-out can be requested.

Websites

Personal data, when released on the Websites, by definition goes beyond the European Economic Area (E.E.A.), including countries that do not have data privacy regimes considered adequate by the EU Commission. The use of personal data in this way should have the consent of the data subject. Where the College uses personal data in this way consideration needs to be given to the reasons for the display of the data.

Web pages that contain personal data about staff / students, such as names, pictures, contact details etc, used for the purposes of the normal functioning and management of the College, should not require the consent of data subjects to be placed on an

institutional Internet or intranet website especially where such information is already available to the public in hardcopy publications such as Calendars and prospectuses. However, staff / students whose personal data is used in this way should be informed of this use, and must still retain the right to object to the use of their data where it would cause them significant damage or distress. The University College can then make a determination on whether the damage or distress alleged is a suitable ground for removal.

All other non-essential uses of personal data on an institutional website, including the use of photographs (background shots, panoramas etc.) where the data subject is clearly identifiable will normally require the institution to make reasonable efforts to ensure that it has obtained the consent of the relevant data subjects.

Where consent is refused, the personal data in question should not be used. If consent cannot be obtained, the University College should consider whether the use of the personal data is likely cause the data subject damage or distress.

Web Pages Used To Collect Personal Data

Where the University College uses web pages to collect personal data, it should ensure that at the point of collection (i.e. on the relevant web page) the following information is provided to the data subject:

- The purpose for which the data is collected
- Those to whom the data is likely to be disclosed
- An indication of the period for which the data will be kept (e.g. "while we process your application", "for the duration of your studies" etc.)
- Any other information that may be required to ensure that the processing is 'fair'.

The data subject should be given the ability to opt out of any parts of the collection of, or use of, the data that are not directly relevant to the intended transaction. (e.g. where an individual provides their name and address to an institution in order to obtain a prospectus, if the institution runs a follow up scheme designed to discover why candidates did not come to that institution, the individual should be notified of that scheme and be able to opt out of it).

Should the University College wish to subsequently use personal data for purposes not disclosed to the data subject at the time of collection, then further consent must be obtained from the individual concerned.

FORWARDING AND REPLYING TO E -MAILS

When forwarding and replying to e-mails all staff and students should consider whether or not those listed on a cc list, intended for their e-mail address to be disclosed to the party you are corresponding with. In particular where e-mails are being forwarded outside the College it is advisable to ensure that those individuals listed in the cc list are happy for their data to be used in this way.