Data Protection Policy May 2018 Onwards: GDPR Compliance

Last Review:	New Policy
Approved by F&GP:	May 2018
Next Review:	July 2019

Vision
Loreto College is centred in God, rooted in Christ and animated by the spirit of Mary Ward, the founder of the Institute of the Blessed Virgin Mary. Our vision is that it will be an educational community where each person has the experience of being loved and valued as a sacred individual created by a loving God; a community where students enjoy an enriching and liberating education that helps them grow into the fullness of life and empowers them to be men and women of courage who are alive to the needs of humanity and committed to making a better world.

Introduction
The College aims to be an educational community which gives expression to the core values of Mary Ward - freedom, justice, sincerity, truth, joy, excellence and internationality.

Loreto College has the highest expectations of personal, academic and professional excellence. This document sets out the steps taken by the college to safeguard personal data. In doing so, the college will be mindful of its core values and of its duty of care to all its staff and students.

1. Purpose and Scope

This Policy sets out the obligations of Loreto College ("the College") regarding data protection and the rights of staff, students and other workers ("data subjects") in respect of their personal data under the General Data Protection Regulation ("the Regulation") from 25th May 2018.

The Regulation defines "personal data" as any information relating to an identified or identifiable natural living person (a 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.

This Policy sets out the procedures that are to be followed when dealing with personal data. The procedures and principles set out herein must be followed at all times by the College, its staff, students, other workers and parties working on behalf of the College.

The Policy applies to all staff, trainees, students, suppliers and others with whom it communicates. Unless otherwise applicable, all references to staff include all current, past, and prospective staff, full time and part time staff as well as agency staff, trainees and contractors. Unless otherwise applicable, all references to students include all current, past and prospective students, whether full-time or part-time.

This Policy does not form part of the terms and conditions of employment for any employee of the College. However, staff are expected to abide by this policy and may be subject to disciplinary procedures if found to be in breach of it.

There are numerous specific data protection terms and phrases used in this Policy. A Glossary of Terms is provided in Appendix 2

.

2. General Policy Statement

In order to operate and to fulfil its legal obligations, the College needs to collect and use certain types of information about people, the data subjects, with whom it deals. These include current, past and prospective students and parents, staff, suppliers, and others with whom it communicates. This personal information must be dealt with properly however it is collected, recorded and used – whether on paper, in a computer, or recorded on other material. All information containing personal data must be protected against unauthorised access, accidental loss or destruction, unintended modification or disclosure.

Individuals conducting the College's business should be aware that any documents they create are viewed as records and the property of the College, and this includes (without limitation) documents, books or leaflets, sheets, reports, correspondence and e-mail including any attachments. Additionally individuals have the same responsibility for managing electronic records as they have for other forms of documents they might produce and the principles of this policy will still apply.

The College regards the lawful and correct treatment of personal information as important to successful operations, and to maintaining confidence between those with whom we deal and the College. To this end the College is committed to the principles of data protection, as stated in the Regulation:

A. processed lawfully, fairly, and in a transparent manner in relation to the data subject

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 will not be considered to be incompatible with the initial purposes

C. adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed

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

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 is processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the Regulation in order to safeguard the rights and freedoms of the data subject

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 organisational measures

The types of information held by the College and how they are used are detailed in the College's registration issued by the Information Commissioner (ICO) under the reference Z6887405. The registration papers are available via the Information Commissioner's Office (ICO) website (www.ico.org.uk) or from the Director of Administration and College Services.

For the College, this means clear policies and procedures for dealing with the control of data which is for both students and staff. The following procedures have been drawn up and staff must be aware of and must follow the requirements as set out in this policy.

Students and staff are made aware of the policy as part of their induction process and periodic staff training events/briefings. Any queries or concerns about this policy or any operational issues which arise should be referred to the Director of Administration and College Services.

Individuals wishing to complain about the College's protection of data should be referred to the College's Complaints Policy.

3. Lawful, Fair, and Transparent Data Processing

The Regulation seeks to ensure that personal data is processed lawfully, fairly, and transparently, without adversely affecting the rights of the data subject. The Regulation states that processing of personal data will be lawful if at least one of the following applies:

a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes

b) processing is necessary for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract

c) processing is necessary for compliance with a legal obligation to which the controller is subject
d) processing is necessary to protect the vital interests of the data subject or of another natural person

e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller

f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child[1]

4. Processed for Specified, Explicit and Legitimate Purposes

4.1 The College collects and processes the personal data set out in Part 21 of this Policy. This may include personal data received directly from data subjects (for example, contact details used when an applicant communicates with us) and data received from third parties (for example, references).

4.2 The College only processes personal data for the specific purposes set out in Part 21 of this Policy (or for other purposes expressly permitted by the Regulation). The purposes for which the College processes personal data will be informed to data subjects at the time that their personal data is collected, where it is collected directly from them, or as soon as possible (not more than one calendar month) after collection where it is obtained from a third party.

5. Adequate, Relevant and Limited Data Processing

The College will only collect and process personal data for and to the extent necessary for the specific purpose(s) informed to data subjects as under Part 4.1, above.

6. Accuracy of Data and Keeping Data Up To Date

The College will ensure that all personal data collected and processed is kept accurate and up-to-date. The accuracy of data will be checked when it is collected and at regular intervals thereafter. Where any inaccurate or out-of-date data is found, all reasonable steps will be taken without delay to amend or erase that data, as appropriate.

7. Timely Processing

The College will not keep personal data for any longer than is necessary in light of the purposes for which that data was originally collected and processed. When the data is no longer required, all reasonable steps will be taken to erase it without delay.

8. Secure Processing

The College will ensure that all personal data collected and processed is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction or damage. Further details of the data protection and organisational measures which will be taken are provided in Parts 22 and 23 of this Policy.

9. Accountability

9.1 The College's Data Protection Officer is Helen Green, the Director of Administration and College Services

9.2 The College will keep written internal records of all personal data collection, holding, and processing, which will incorporate the following information:

a) The name and details of the College, its Data Protection Officer, and any applicable third party data controllers

b) The purposes for which the College processes personal data

c) Details of the categories of personal data collected, held, and processed by the College; and the categories of data subject to which that personal data relates

d) Details (and categories) of any third parties that will receive personal data from the College

e) Details of any transfers of personal data to non-EEA countries including all mechanisms and security safeguards

f) Details of how long personal data will be retained by the College

g) Detailed descriptions of all technical and organisational measures taken by the College to ensure the security of personal data

10. Privacy Impact Assessments

The College will carry out Privacy Impact Assessments when and as required under the Regulation. Privacy Impact Assessments will be overseen by the College's Data Protection Officer and will address the following areas of importance:

a) The purpose(s) for which personal data is being processed and the processing operations to be carried out on that data

b) Details of the legitimate interests being pursued by the College

c) An assessment of the necessity and proportionality of the data processing with respect to the purpose(s) for which it is being processed

d) An assessment of the risks posed to individual data subjects

e) Details of the measures in place to minimise and handle risks including safeguards, data security, and other measures and mechanisms to ensure the protection of personal data, sufficient to demonstrate compliance with the Regulation.

11. The Rights of Data Subjects

The Regulation sets out the following rights applicable to data subjects. These rights are subject to compliance with other legal and business requirements.

a) The right to be informed

b) The right of access

c) The right to rectification

d) The right to erasure (also known as the 'right to be forgotten')

e) The right to restrict processing

f) The right to data portability

g) The right to object

h) Rights with respect to automated decision-making and profiling.

12. Keeping Data Subjects Informed

12.1 The College will ensure that the following information is provided to every data subject when personal data is collected:

a) Details of the College including, but not limited to, the identity of Helen Green, the College's Data Protection Officer

b) The purpose(s) for which the personal data is being collected and will be processed (as detailed in Part 21 of this Policy) and the legal basis justifying that collection and processing

c) Where applicable, the legitimate interests upon which the College is justifying its collection and processing of the personal data

d) Where the personal data is not obtained directly from the data subject, the categories of personal data collected and processed

e) Where the personal data is to be transferred to one or more third parties, details of those parties

f) Where the personal data is to be transferred to a third party that is located outside of the European Economic Area (the "EEA"), details of that transfer, including but not limited to the safeguards in place (see Part 24 of this Policy for further details concerning such third country data transfers)

g) Details of the length of time the personal data will be held by the College (or, where there is no predetermined period, details of how that length of time will be determined)

h) Details of the data subject's rights under the Regulation

i) Details of the data subject's right to withdraw their consent to the College's processing of their personal data at any time

j) Details of the data subject's right to complain to the Information Commissioner's Office (the 'supervisory authority' under the Regulation)

k) Where applicable, details of any legal or contractual requirement or obligation necessitating the collection and processing of the personal data and details of any consequences of failing to provide it

l) Details of any automated decision-making that will take place using the personal data (including but not limited to profiling), including information on how decisions will be made, the significance of those decisions and any consequences.

12.2 The information set out above in Part 12.1 shall be provided to the data subject at the following applicable time:

12.2.1 Where the personal data is obtained from the data subject directly, at the time of collection

12.2.2 Where the personal data is not obtained from the data subject directly (i.e. from another party):

a) if the personal data is used to communicate with the data subject, at the time of the first communication, or

b) if the personal data is to be disclosed to another party, before the personal data is disclosed, or

c) in any event, not more than one month after the time at which the College obtains the personal data.

13. Data Subject Access

13.1 A data subject may make a subject access request ("SAR") at any time to find out more about the personal data which the College holds about them. The College is normally required to respond to SARs within one month of receipt (this can be extended by up to two months in the case of complex and/or numerous requests, and in such cases the data subject shall be informed of the need for the extension).

13.2 All subject access requests received must be forwarded to:

Data Protection Officer
Loreto College
Chichester Road South
Hulme
Manchester
M15 5PB

Email: dpo@loreto.ac.uk

13.3 The College does not charge a fee for the handling of normal SARs. The College reserves the right to charge reasonable fees for additional copies of information that have already been supplied to a data subject, and for requests that are manifestly unfounded or excessive, particularly where such requests are repetitive.

14. Rectification of Personal Data

14.1 If a data subject informs the College that personal data held by the College is inaccurate or incomplete, requesting that it be rectified, the personal data in question will be rectified, and the data subject informed of that rectification, within one month of receipt of the data subject's notice (this can be extended by up to two months in the case of complex requests, and in such cases the data subject shall be informed of the need for the extension).

14.2 In the event that any affected personal data has been disclosed to third parties, those parties will be informed of any rectification of that personal data.

14.3. The College will, undertake regular data checking with staff and students as follows:

- Students: biographical and contact details will be checked each term through the Personal Tutor programme
- Staff: biographical and contact details will be checked annually

In addition, students, parents and staff are provided with secure online access to this (and other information) via:

- Students: myLoreto
- Parents: Parent Portal
- Staff: myLoreto/Columbus

15. Erasure of Personal Data

15.1 Data subjects may request that the College erases the personal data it holds about them in the following circumstances:

a) it is no longer necessary for the College to hold that personal data with respect to the purpose for which it was originally collected or processed

b) the data subject wishes to withdraw their consent to the College holding and processing their personal data

c) the data subject objects to the College holding and processing their personal data (and there is no overriding legitimate interest to allow the College to continue doing so) (see Part 18 of this Policy for further details concerning data subjects' rights to object)

d) the personal data has been processed unlawfully

e) the personal data needs to be erased in order for the College to comply with a particular legal obligation

15.2 Unless the College has reasonable grounds to refuse to erase personal data, all requests for erasure shall be complied with, and the data subject informed of the erasure, within one month of receipt of the data subject's request (this can be extended by up to two months in the case of complex requests, and in such cases the data subject will be informed of the need for the extension).

15.3 In the event that any personal data that is to be erased in response to a data subject request has been disclosed to third parties, those parties will be informed of the erasure (unless it is impossible or would require disproportionate effort to do so).

16. Restriction of Personal Data Processing

16.1 Data subjects may request that the College ceases processing the personal data it holds about them. If a data subject makes such a request, the College will retain only the amount of personal data pertaining to that data subject that is necessary to ensure that no further processing of their personal data takes place.

16.2 In the event that any affected personal data has been disclosed to third parties, those parties will be informed of the applicable restrictions on processing it (unless it is impossible or would require disproportionate effort to do so).

17. Data Portability

17.1 Where data subjects have given their consent to the College to process their personal data in such a manner or the processing is otherwise required for the performance of a contract between the College and the data subject, data subjects have the legal right under the Regulation to receive a copy of their personal data and to use it for other purposes (namely transmitting it to other data controllers, e.g. other Colleges).

17.2 To facilitate the right of data portability, the College shall make available all applicable personal data to data subjects in the comma separated values (.csv) format

17.3 Where technically feasible, if requested by a data subject, personal data will be sent directly to another data controller, using suitable encryption.

17.4 All requests for copies of personal data shall be complied with within one month of the data subject's request (this can be extended by up to two months in the case of complex requests in the case of complex or numerous requests, and in such cases the data subject shall be informed of the need for the extension).

18. Objections to Personal Data Processing

18.1 Data subjects have the right to object to the College processing their personal data based on legitimate interests (including profiling), direct marketing (including profiling), and processing for scientific and/or historical research and statistical purposes.

18.2 Where a data subject objects to the College processing their personal data based on its legitimate interests, the College will cease such processing forthwith, unless it can be demonstrated that the College's legitimate grounds for such processing override the data subject's interests, rights and freedoms; or the processing is necessary for the conduct of legal claims.

18.3 Where a data subject objects to the College processing their personal data for direct marketing purposes, the College will cease such processing forthwith.

18.4 Where a data subject objects to the College processing their personal data for scientific and/or historical research and statistical purposes, the data subject must, under the Regulation, 'demonstrate grounds relating to his or her particular situation'. The College is not required to comply if the research is necessary for the performance of a task carried out for reasons of public interest.

19. Automated Decision-Making

19.1 In the event that the College uses personal data for the purposes of automated decision-making and those decisions have a legal (or similarly significant effect) on data subjects, data subjects have the right to challenge such decisions under the Regulation, requesting human intervention, expressing their own point of view, and obtaining an explanation of the decision from the College.

19.2 The right described in Part 19.1 does not apply in the following circumstances:

a) The decision is necessary for the entry into, or performance of, a contract between the College and the data subject

b) The decision is authorised by law or

c) The data subject has given their explicit consent

The College does not currently employ automated decision-making systems.

20. Profiling

In the event that the College uses personal data for profiling purposes, the following shall apply:

a) Clear information explaining the profiling will be provided, including its significance and the likely consequences

b) Appropriate mathematical or statistical procedures will be used

c) Technical and organisational measures necessary to minimise the risk of errors and to enable such errors to be easily corrected shall be implemented and

d) All personal data processed for profiling purposes shall be secured in order to prevent discriminatory effects arising out of profiling (see Parts 22 and 23 of this Policy for more details on data security).

The College does not currently employ profiling systems.

21. Personal Data (including Retention Periods)

The following personal data may be collected, held, and processed by the College:

Staff Data

Type of Data	***Retention Period***	***Reason***
Personal data including: *Date of Birth (hence Age)* *Gender* *Ethnic origin* *Disabilities* *Religion (where declared)* *Education and qualifications gained* *Previous employment history* *References from previous employers*	*10 years after member of staff leaves*	*Safer recruitment legislation* *Equality and Diversity monitoring* *Insurance Requirements*

Results of groups taught prior to appointment *Address and contact details* *Absences and reasons for absence* *DBS details and any convictions* *Pregnancy* *Health issues* *Photograph* *Professional development reviews*		*Health & Safety regulations* *Welfare and support*
Pension Details	*72 years from birth or five years after retirement, whichever is longer*	
Application forms	*Six months*	*Litigation*
Redundancy facts	*12 years from date of redundancy*	*Litigation*
Income tax and NI	*6 years from the end of the financial year to which they relate*	*Income Tax [Employment] Regulations 1993*
Maternity pay	*6 years from the end of the financial year to which they relate* *6 years*	*Statutory Maternity Pay [General] Regulations 1986*
Statutory sick pay		*Statutory Sick Pay [General] Regulations 1982*
Wages and salaries		*Taxes Management Act 1970*
Accident books etc	*3 years after the date of last entry*	*Social Security (Claims and Payments) Regulations 1979, RIDDOR 1985*
Health records where termination of employment is related to, and Medical records relating to, Control of Substances Hazardous to Health	*40 years from date of last entry*	*COSHH 1999*
Ionising Radiation Records	*50 years after last entry*	*Ionising Radiation Regulations 1985*
Health records where termination of employment is due to asbestos-related illness	*50 years*	*Control of Asbestos at work Regulations 1987*
Disciplinary records	*Details of any disciplinary matters will be removed from staff files after a length of time recorded at the disciplinary hearing* ***but*** *a copy of the lapsed warning will be kept as a part of an accurate record of the employment relationship.*	

Student Data

Computerised data	***Retention Period***	***Reason***
Personal data including: *Date of Birth (hence Age)* *Gender* *Ethnic origin*	*10 years after student leaves*	*To provide education under the Education Act (1992)*

Disabilities *Religion (where declared)* *Learning difficulties* *Also, in some cases:* *Family income (Bursary applicants)* *DBS details* *Pregnancy* *Health issues* *For all students:* *Country of domicile* *Qualifications on entry (all applicants)* *Address and contact details* *Previous school* *Courses applied for* *Courses taken (with dates)* *Attendance* *Reasons for absence* *Assessment marks* *Reviews of progress* *Final results* *Disciplinary matters* *Careers advice* *Subject and Personal Tutor References* *Photograph*		*Bursary allocation* *Safeguarding regulations* *Health & Safety regulations* *Welfare and support*
Forms and other material		
Enrolment forms *Amendment forms* *Registers*	*10 years after completion of course*	*Audit requirements* *Inspection*
Student disciplinary records *Welfare forms*	*10 years after completion of course*	*Possible litigation* *Inspection*
Coursework marks *Student concern records* *Risk assessments*	*One year after end of course*	*Appeals* *Inspection*
Student Work	*As required by relevant awarding bodies.*	*Internal and external verification* *Student appeals* *Internal and external inspection*
Application forms for non-enrolees	*18 months after application closing date*	*Reference for re-applications*
Reasons for bursary payment decisions	*Six years after the student completes course*	*Audit requirements*
Uncollected Examination Certificates	*12 months after issue* *(Record of destroyed certificates will be kept for four years)* *Returned to Exam Boards*	*JCQ Guidance*
Safeguarding records	*Until the subject reaches the age of 25 years*	*Safeguarding guidance*

General Data

Type of Data	***Retention Period***	***Reason***
Professional Advice Records e.g. Careers, Personnel	*Kept as long as is necessary to open and process a case and for five years from case closure*	*Necessary for processing and potential follow on queries*
CCTV footage	*30 days (unless there are any incidents which are kept securely until resolved)*	*Security of staff, students, visitors and property. Safeguarding.*
Internet Monitoring Records	*Up to 12 months*	*Ensuring facilities are used within guideline. Safeguarding.*

22. Data Protection Measures

The College will ensure that all its employees, agents, contractors, or other parties working on its behalf comply with the following when working with personal data:

a) All Governors, staff and students will have their own individual log-in and password for access to the network. Staff and student responsibilities with regard to their network accounts are outlined above and in the College's IT User Agreements.

b) There are separate staff logins for access to UNITe, Columbus and myLoreto (student data), staff should not share logins to either the network or the UNITe/Columbus system. If personal data is being viewed on a computer screen and the computer in question is to be left unattended for any period of time, the user must lock the computer and screen before leaving it. Teachers should pay particular care in class and freeze the data projector screen if accessing email, UNITe/Columbus/myLoreto or other non-teaching systems/files.

c) Emails containing personal data eg HR records must be encrypted

d) Where any personal data is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed), it should be securely deleted and disposed of. Hardcopies should be shredded, and electronic copies should be deleted securely using software provided by the College.

e) Personal data may be transmitted over secure networks only; transmission over unsecured networks is not permitted in any circumstances.

f) Personal data may not be transmitted over a wireless network if there is a wired alternative that is reasonably practicable.

g) Personal data contained in the body of an email, whether sent or received, should be either: copied from the body of that email into an encrypted Word file (See Appendix 9) and stored securely or printed and stored securely. The email itself should be deleted. All temporary files associated therewith should also be deleted. Note: the email deleted items folder should also be "purged" (See Appendix 9) after the file has been deleted to prevent recovery of the file.

h) Where Personal data is to be sent by facsimile transmission the recipient should be informed in advance of the transmission and should be waiting by the fax machine to receive the data.

i) Where Personal data is to be transferred in hardcopy form it should be passed directly to the recipient or sent using Royal Mail Special Delivery (signed for).

j) No personal data may be shared informally and if an employee, agent, sub-contractor, or other party working on behalf of the College requires access to any personal data that they do not already have access to, then a third party agreement should be in place.

k) No personal data may be transferred to any employees, agents, contractors, or other parties, whether such parties are working on behalf of the College or not, without the authorisation of Helen Green.

l) All hardcopies of personal data, along with any electronic copies stored on physical, removable media (CD, DVD or external disk/pen drive) should be stored securely in a locked box, drawer, cabinet or similar.

m) Personal data must be handled with care at all times and should not be left unattended or on view to students, unauthorised employees, agents, sub-contractors or other parties at any time.

n) No personal data should be stored on any mobile device (including, but not limited to, laptops, tablets and smartphones), whether such device belongs to the College or otherwise without the formal written approval of the Principal, and, in the event of such approval, strictly in accordance with all instructions and limitations described at the time the approval is given, and for no longer than is absolutely necessary.

o) If personal data needs to be transferred to any device personally belonging to an employee then it is subject to the same security requirements as a college device. Personal data may only be transferred to devices belonging to agents, contractors, or other parties working on behalf of the College where the party in question has agreed to comply fully with the letter and spirit of this Policy and of the Regulation (which may include demonstrating to the College that all suitable technical and organisational measures have been taken).

p) All personal data stored electronically should be backed up daily with backups stored onsite. All backups should be encrypted.

q) All electronic copies of personal data should be stored securely using passwords and data encryption (See Appendix 9)

r) All passwords used to protect personal data should be changed regularly and should not use words or phrases that can be easily guessed or otherwise compromised. See the College Password Standard Policy.

s) Under no circumstances should any personal passwords be written down or shared between any employees, agents, contractors, or other parties working on behalf of the College, irrespective of seniority or department. If a password is forgotten, it must be reset using the applicable method. IT staff do not have access to passwords

t) Where personal data held by the College is used for marketing purposes, no data will be added to any marketing preference databases including, but not limited to, the Telephone Preference Service, the Mail Preference Service, the Email Preference Service, and the Fax Preference Service.

u) The computerised CCTV recordings are considered as personal data under the Regulation. Recordings on the CCTV files will only be used by the College for security purposes, including in-house investigation and for liaison with the police for serious or criminal incidents. In these cases, copies of recordings and prints can be retained for up to 6 years where criminal proceedings are possible. Otherwise, recordings are permanently erased on a rolling basis within 30 days.

23. Organisational Measures

The College will ensure that the following measures are taken with respect to the collection, holding, and processing of personal data:

a) All employees, agents, contractors, or other parties working on behalf of the College will be made fully aware of both their individual responsibilities and the College's responsibilities under the Regulation and under this Policy, and will be provided with a copy of this Policy

b) Only employees, agents, sub-contractors, or other parties working on behalf of the College that need access to, and use of, personal data in order to carry out their assigned duties correctly will have access to personal data held by the College

c) All employees, agents, contractors, or other parties working on behalf of the College handling personal data will be appropriately trained to do so

d) All employees, agents, contractors, or other parties working on behalf of the College handling personal data will be appropriately supervised

e) Methods of collecting, holding and processing personal data will be regularly evaluated and reviewed

f) The performance of those employees, agents, contractors, or other parties working on behalf of the College handling personal data will be regularly evaluated and reviewed

g) All employees, agents, contractors, or other parties working on behalf of the College handling personal data will be bound to do so in accordance with the principles of the Regulation and this Policy by contract

h) All agents, contractors, or other parties working on behalf of the College handling personal data must ensure that any and all of their employees who are involved in the processing of personal data are held to the same conditions as those relevant employees of the College arising out of this Policy and the Regulation

i) Where any agent, contractor or other party working on behalf of the College handling personal data fails in their obligations under this Policy that party will indemnify and hold harmless the College against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

24. Transferring Personal Data to a Country Outside the EEA

24.1 The College may from time to time transfer ('transfer' includes making available remotely) personal data to countries outside of the EEA.

24.2 The transfer of personal data to a country outside of the EEA shall take place only if one or more of the following applies:

a) The transfer is to a country, territory, or one or more specific sectors in that country (or an international organisation), that the European Commission has determined ensures an adequate level of protection for personal data

b) The transfer is to a country (or international organisation) which provides appropriate safeguards in the form of a legally binding agreement between public authorities or bodies; binding corporate rules; standard data protection clauses adopted by the European Commission; compliance with an approved code of conduct approved by a supervisory authority (e.g. the Information Commissioner's Office); certification under an approved certification mechanism (as provided for in the Regulation); contractual clauses agreed and authorised by the competent supervisory authority; or provisions inserted into administrative arrangements between public authorities or bodies authorised by the competent supervisory authority.

   NB: The EU-US Privacy Shield scheme became operational on 1 August 2016 after the European Commission issued its formal decision that the Privacy Shield provides adequate protection to allow personal data to be transferred to the United States.

c) The transfer is made with the informed consent of the relevant data subject(s)

d) The transfer is necessary for the performance of a contract between the data subject and the College

e) The transfer is necessary for important public interest reasons

f) The transfer is necessary for the conduct of legal claims

g) The transfer is necessary to protect the vital interests of the data subject or other individuals where the data subject is physically or legally unable to give their consent

h) The transfer is made from a register that, under UK or EU law, is intended to provide information to the public and which is open for access by the public in general or otherwise to those who are able to show a legitimate interest in accessing the register.

25. Data Breach Notification

25.1 All personal data breaches must be reported immediately to Helen Green, the College's Data Protection Officer who will inform Loreto College, the Data Controller.

25.2 If a personal data breach occurs that is likely to result in a risk to the rights and freedoms of data subjects (e.g. breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the Data Controller must ensure that the Information Commissioner's Office is informed of the breach without delay, and in any event, within 72 hours after having become aware of it.

25.3 In the event that a personal data breach is likely to result in a high risk (that is, a higher risk than that described under Part 25.2) to the rights and freedoms of data subjects, the Data Controller must ensure that all affected data subjects are informed of the breach directly and without undue delay.

25.4 Data breach notifications shall include the following information:

a) The categories and approximate number of data subjects concerned

b) The categories and approximate number of personal data records concerned

c) The name and contact details of the College's Data Protection Officer (or other contact point where more information can be obtained)

d) The likely consequences of the breach

e) Details of the measures taken, or proposed to be taken, by the College to address the breach including, where appropriate, measures to mitigate its possible adverse effects

Infringement of the EU General Data Protection Regulations can result in administrative fines of up to 4% of annual global turnover or €20 million - whichever is greater.

26. Implementation of Policy

This Policy will be deemed effective as of 25 May 2018. No part of this Policy will have retroactive effect and shall thus apply only to matters occurring on or after this date.

Approved in principle, by the Finance & General Purposes Committee on 9th May 2018, for recommendation to the Governing Body.

Related Policies

CCTV Policy
Examinations Procedures
Freedom of Information Policy
Staff Code of Conduct

Appendix 1: Roles and Responsibilities in relation to Data Protection

Governors

As the employer, the Governing Body is responsible for establishing and reviewing the College's Data Protection Policy.

Principal

The Principal is responsible for arranging the delegated responsibility for:

- ensuring that the College has a Data Protection Policy compliant with the Regulations
- authorisation of access to the Human Resources (HR) system and paper based staff records.
- authorising appropriate staff access to the HR and Payroll systems
- authorising requests for the disclosure of images from the CCTV system

Director of Administration and College Services

Acts as the College's Data Protection Officer (DPO) and is responsible for:

- the day to day implementation, review and development of this policy
- staff training on GDPR
- renewal of the College's registration with the ICO
- reporting Data Protection breaches to the ICO
- ensuring that data access requests are processed appropriately

Deputy Principal (Student Services)

is responsible for the:

- secure creation, maintenance and destruction of safeguarding records
- liaising with other agencies in connection with safeguarding
- secure creation, maintenance and destruction of student medical support plans
- management of the counsellors and their Data Protection procedures

The Head of Information Systems

is responsible for the:

- management and security of the College IT systems
- appropriate operation of the CCTV system

The College Accountant

is responsible for:

- controlling appropriate staff access to the Finance System
- secure creation, maintenance and destruction of information relating to financial records

The HR Manager

is responsible for the:

- secure creation, maintenance and destruction of information relating to staff applicants, staff members, agency staff and trainees
- controlling appropriate access to staff information

The CIS Manager

is responsible for the:

- secure creation, maintenance and destruction of information relating to students

The Learning Support Manager

Is responsible for:

- the secure creation, maintenance and destruction of learning support and examination access records

The Counsellors

are responsible for the secure creation, maintenance and destruction of counselling records

The Work Placement Officer

is responsible for the collation of the Work Experience Consent and Placement Form and its sharing with the work placement organisation.

All Staff

are responsible for:

- checking that any information that they provide to the College in connection with their employment is accurate and up to date
- informing the College of any changes to information, which they have provided e.g. change of address
- checking the information that the College will send out from time to time, giving details of information kept and processed about staff
- informing the College of any errors, changes or omissions
- abiding by the guidance in this, or other relevant polices or procedures
- ensuring the security of their network login and password
- not leaving network systems logged in, unattended or openly displaying sensitive information
- logging off from network systems after use
- any personal information that they keep is secure and not disclosed either orally or in writing or accidentally to any unauthorised third party.

Students

are responsible for:

- checking that any information that they provide to the College in connection with their education is accurate and up to date
- informing the College of any changes to information, which they have provided e.g. change of address
- checking the information that the College will send out from time to time, giving details of information kept and processed about students
- informing the College of any errors, changes or omissions

Appendix 2: Data Protection Glossary

Data Protection legislation uses a number of technical terms that you should be aware of.

Consent

Any freely given specific and informed indication of his or her wishes by which the data subject signifies his or her agreement to personal data relating to him or her being processed. Consent can be withdrawn after it has been given.

Where data is 'sensitive', express consent must be given for processing this data.

Data Controller

Person, company or organisation who determines the purpose and manner of the processing of personal data, in other words, the body responsible for the data (i.e. Loreto College).

Data Processor

Any person (other than an employee of the data controller), company or organisation who processes the data on behalf of the data controller (e.g. an Awarding Body processes student examination entries or a pensions provider for staff).

Data processing

Obtaining, recording or holding (storing) information and carrying out any operation or set of operations upon it, including:

- adaptation
- alteration
- retrieval
- consultation
- use
- disclosure
- transfer
- erasure
- destruction

Data Subject

Any living individual who is the subject of personal data.

Secondary Data Subject

A second data subject whose data may be processed in relation to the Data Subject e.g. a student's parental contact details, a member of staff's next of kin.

Data Subject Access Request (SAR)

The right of an individual to inspect all personal data relating to him or her held by a data controller. The data controller must produce the requested information in an intelligible and, unless this is impracticable, permanent format.

DIN

DIN refers to the Deutsches Institut für Normung eV or German Institute for Standardization. It is a standard that helps qualify "Data Destruction" security levels used in Europe. DIN 3 has maximum permitted strip width 2mm or max particle size 4 x 30mm. The minimum security level for disposing of highly personal documents. The recommended minimum security level for sensitive business information such as customer information, accounts and marketing data, draft plans, personnel records etc.

Encryption

Is a means of preventing anyone other than those who have a key from accessing data, be it in an email or attachment, a file on a PC or a storage device. Contact Network Services for information.

European Economic Area (EEA)

Personal data should not normally be transferred outside the European Economic Area (EEA). The EEA comprises of the following countries: Austria, Belgium, Bulgaria, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden and the United Kingdom.

NB: The EU-US Privacy Shield scheme became operational on 1 August 2016 after the European Commission issued its formal decision that the Privacy Shield provides adequate protection to allow personal data to be transferred to the United States.

Mobile devices

Where we refer to 'mobile devices', the definition is intended to be broad and includes memory sticks, mobile phones, tablets, PDAs, netbooks and laptops.

Personal data

Information relating to a named or otherwise identifiable individual. This includes any expressions of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

Profiling

The GDPR defines profiling as any form of automated processing intended to evaluate certain personal aspects of an individual, in particular to analyse or predict their:

- performance at work
- economic situation
- health
- personal preferences
- reliability
- behaviour
- location
- movements

Protected Characteristics

The Equality Act (2010) defines the following nine protected characteristics:

- age
- disability
- gender reassignment
- marriage and civil partnership
- pregnancy and maternity
- race
- religion or belief
- sex
- sexual orientation

Readily Accessible Filing System

The ICO defines a readily accessible filing system as one that a temporary administrative assistant (a 'temp') would be able to extract specific information about an individual from manual records without any particular knowledge of the College's type of work or the documents held.

This 'temp test' assumes that the temp in question is reasonably competent, requiring only a short induction, explanation and/or operating manual on the particular filing system in question for them to be able to use it.

Recipient

Under the Data Protection Act, a recipient is defined as any person to whom the data are disclosed, including any person to whom they are disclosed in the course of processing the data for the Data Controller (for example, an employee of the data controller, a data processor or employee of the data processor).

Sensitive personal data

Personal data containing information relating to the racial or ethnic origin, political opinions, religious beliefs, trade union membership, physical or mental health, sexual life, alleged or actual criminal history of a data subject.

The College also classifies family circumstance and income as sensitive personal data.

Text Data

Information held in text form about an individual.

Non-Text Data

Image, CCTV footage, still images, audio, biometric (e.g. finger-print), location data from which an individual can be identified.

Third party

The Data Protection Act defines a 'third party', in relation to personal data, as any person other than:

- the data subject
- the data controller
- any data processor or other person authorised to process data for the data controller or processor
- 'Third party' does not include employees or agents of the data controller or data processor.