Examinations
General Data Protection Regulation Policy

Reviewed January 2020

1. AIMS

1.1 To be a Catholic school where all members of the community live according to Gospel values and the principles and teachings of Mary Ward, promoting the virtues of freedom, sincerity, justice, truth and joy, to allow all members of the community to feel secure and able to work and live in an atmosphere of courtesy and respect.

1.2 To create a caring and stable environment, in which each person is respected as an individual with unique gifts, talents and ambitions, and is given the freedom and confidence to develop these.

2. GUIDING PRINCIPLES

2.1 The Governors and School appreciate the responsibility of running an exam centre and to this end adopt the policies suggested by JCQ.

3. CONTENTS

4. PURPOSE OF THE POLICY

4.1 This policy details how Loreto College, in relation to exams management and administration, ensures compliance with the regulations as set out by the Data Protection Act 2018 (DPA 2018) and General Data Protection Regulation (GDPR).

Students are given the right to find out what information the centre holds about them, how this is protected, how this can be accessed and how data breaches are dealt with.

All exams office staff responsible for collecting and sharing candidates' data are required to follow strict rules called 'data protection principles' ensuring the information is:

- used fairly and lawfully;
- used for limited, specifically stated purposes;
- used in a way that is adequate, relevant and not excessive;
- accurate;
- kept for no longer than is absolutely necessary;
- handled according to people's data protection rights;
- kept safe and secure;
- not transferred outside the European Economic Area without adequate protection.

To ensure that the centre meets the requirements of the DPA 2018 and GDPR, all candidates' exam information – even that which is not classified as personal or sensitive – is covered under this policy.

5. EXAMS RELATED INFORMATION

5.1 There is a requirement for the exams officer to hold exams-related information on candidates taking external examinations. For further details on the type of information held please refer to Section 8.

Candidates' exams-related data may be shared with the following organisations:

- Awarding bodies;
- Joint Council for Qualifications;
- Department for Education;
- Local Authority;
- Other Schools in the Consortium.

This data may be shared via one or more of the following methods:

- hard copy;
- email;
- secure extranet sites e.g. eAQA, OCR Interchange, Pearson Edexcel Online and WJEC Secure services;
- Management Information System (MIS) provided Capita SIMS sending/receiving information via electronic data interchange (EDI) using A2C.

This data may relate to exam entries, access arrangements, the conduct of exams and non-examination assessments, special consideration requests and exam results/post-results/certificate information.

6. INFORMING CANDIDATES OF THE INFORMATION HELD

6.1 Loreto College ensures that candidates are fully aware of the information and data held. All candidates are:

- informed via a letter before the examination series begins;
- given access to this policy via the Loreto website.

Candidates are made aware of the above in the spring term leading to an externally accredited qualification.

At this point, the centre also brings to the attention of candidates the annually updated JCQ document Information for candidates – Privacy Notice which explains how the JCQ awarding bodies process their personal data in accordance with the DPA 2018 and GDPR.

Candidates eligible for access arrangements are also required to provide their consent by signing the GDPR compliant JCQ candidate personal data consent form (Personal data consent, Privacy Notice (AAO) and Data Protection confirmation) before access arrangements approval applications can be processed online.

7. DEALING WITH DATA BREACHES

7.1 Although data is handled in line with DPA/GDPR regulations, a data breach may occur for any of the following reasons:

- loss or theft of data or equipment on which data is stored;
- inappropriate access controls allowing unauthorised use;
- equipment failure;
- human error;
- unforeseen circumstances such as a fire or flood;
- hacking attack;
- 'blagging' offences where information is obtained by deceiving the organisation who holds it.

If a data protection breach is identified, the following steps will be taken:

7.2 1) Containment and Recovery

7.2.1 The Data Protection Officer will lead on investigating the breach.
It will be established:

- who needs to be made aware of the breach and inform them of what they are expected to do to assist in the containment exercise. This may include isolating or closing a compromised section of the network, finding a lost piece of equipment and/or changing the access codes;
- whether there is anything that can be done to recover any losses and limit the damage the breach can cause. As well as the physical recovery of equipment, this could involve the use of back-up hardware to restore lost or damaged data or ensuring that staff recognise when someone tries to use stolen data to access accounts;
- which authorities, if relevant, need to be informed.

7.3 2) Assessment of ongoing risk

7.3.1 The following points will be considered in assessing the ongoing risk of the data breach:

- what type of data is involved?
- how sensitive is it?
- if data has been lost or stolen, are there any protections in place such as encryption?
- what has happened to the data? If data has been stolen, it could be used for purposes which are harmful to the individuals to whom the data relates; if it has been damaged, this poses a different type and level of risk;
- regardless of what has happened to the data, what could the data tell a third party about the individual?
- how many individuals' personal data are affected by the breach?
- who are the individuals whose data has been breached?
- what harm can come to those individuals?
- are there wider consequences to consider such as a loss of public confidence in an important service we provide?

7.4 3) Notification of breach

7.4.1 Notification will take place to enable individuals who may have been affected to take steps to protect themselves or to allow the appropriate regulatory bodies to perform their functions, provide advice and deal with complaints.

7.5 4) Evaluation and response

7.5.1 Once a data breach has been resolved, a full investigation of the incident will take place. This will include:

- reviewing what data is held and where and how it is stored;
- identifying where risks and weak points in security measures lie (for example, use of portable storage devices or access to public networks);
- reviewing methods of data sharing and transmission;
- increasing staff awareness of data security and filling gaps through training or tailored advice;
- reviewing contingency plans.

8. ACCESS TO INFORMATION

8.1 Current and former candidates can request access to the information/data held on them by making a subject access request to the Examinations Officer in writing or email and how ID will need to be confirmed if a former candidate is unknown to current staff. All requests will be dealt with within 40 calendar days.

8.2 Third Party access

8.2.1 Permission should be obtained before requesting personal information on another individual from a third-party organisation.

Candidates' personal data will not be shared with a third party unless a request is accompanied with permission from the candidate and appropriate evidence (where relevant), to verify the ID of both parties, provided.

In the case of looked-after children or those in care, agreements may already be in place for information to be shared with the relevant authorities (for example, the Local Authority). The centre's Designated Senior Person for Child Protection will confirm the status of these agreements and approve/reject any requests.

8.3 Publishing exam results

8.3.1 Exam results will be provided to the student directly unless written permission is provided by the student. Exam results published online will only be done in an anonymous fashion so students cannot be identified unless permission is given by the students.

9. **TABLE RECORDING CANDIDATE EXAMS-RELATED INFORMATION HELD**

Information type	What personal/sensitive data is/may be contained in the information	Where information is stored	How information is protected	Retention period
Access arrangements information	Candidate name Candidate DOB Gender Data protection notice (candidate signature) Diagnostic testing outcomes Specialist reports Evidence of normal way of working	Access Arrangements Online MIS provided by Capita SIMS Lockable metal filing cabinet	Secure user name and password In secure area solely assigned to storing access arrangements information	For 10 years after the candidate has left the School
Attendance registers copies	Candidate name Candidate Number	Examination Secure Storage	In Secure Storage only accessible by Exams Office and Head of Centre	Until all reviews of results are completed
Candidates' scripts	Candidate name Candidate number Candidate's work	Examination Secure Storage until collected by courier company	In Secure Storage only accessible by Exams Office and Head of Centre	Up to one day until collected by courier company
Certificates	Candidate name Candidate number	Filing cabinet in exams office, filed in main reception office (When ready to be collected) or in the locked archive room.	All rooms are locked when selected personal are not inside	Until collected by the student.
Certificate issue information	Candidate name Candidate signature	In the main office with certificates to be collected.	The office is only accessed by selected personal and locked when empty.	Until all certificates have been collected.
Entry information	Candidate name Candidate DOB Gender Candidate number	MIS provided by Capita SIMS	Secure user name and password	Retained while student is on SIMs

Information type	What personal/sensitive data is/may be contained in the information	Where information is stored	How information is protected	Retention period
Exam room incident logs	Candidate name Candidate number Details of the incident	Examination Secure Storage	In Secure Storage only accessible by Exams Office and Head of Centre	Until all reviews of results are completed
Invigilator and facilitator training records	Invigilator name Date of training	Examination officers personal computer drive	Secure user name and password	Until all reviews of results are completed
Post-results services: confirmation of candidate consent information	Candidate name Candidate number Candidate signature	Filing cabinet in exams office	All rooms are locked when selected personal are not inside	Until all reviews of results are completed
Post-results services: requests/outcome information	Candidate name Candidate number Candidate exam result	MIS provided by Capita SIMS Examination Boards secure website	Secure user name and password	For 1 year after the examination series is compete
Post-results services: scripts provided by ATS service	Candidate name Candidate number	For scripts requested by students the information is not retained. For scripts used for teaching and learning the personal data is removed	Information is removed or passed on to the candidate	N/A
Private candidate information	Candidate name Candidate number Candidate DOB Candidate address Candidate phone number	MIS provided by Capita SIMS	Secure user name and password	For 10 years after the candidate has left the School
Results information	Candidate name Candidate number Candidate DOB Candidate exam results	MIS provided by Capita SIMS	Secure user name and password	For 10 years after the candidate has left the School
Seating plans	Candidate name Candidate number	Examination Secure Storage	In Secure Storage only accessible by	Until all reviews of results are

Information type	What personal/sensitive data is/may be contained in the information	Where information is stored	How information is protected	Retention period
	Access arrangement information		Exams Office and Head of Centre	completed
Special consideration information	Candidate name Candidate number Reason for request	MIS provided by Capita SIMS Examination boards secure website	Secure user name and password	Until all reviews of results are completed
Very late arrival reports/outcomes	Candidate name Candidate number Reason for late arrival	Examination boards secure website	Secure user name and password	Until all reviews of results are completed