St Richard's Catholic College

DATA PROTECTION POLICY FOR EXAMS

The Policy was approved by the Governing Body: October 2022

Chair of Governors:

The Governing Body will review the policy in October 2023

Purpose of the policy

This policy details how St Richard's Catholic 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 UK General Data Protection Regulation (GDPR).

The delivery of examinations and assessments involve centres and awarding bodies processing a significant amount of personal data (i.e. information from which a living individual might be identified). It is important that both centres and awarding bodies comply with the requirements of the UK General Data Protection Regulation and the Data Protection Act 2018 or law relating to personal data in any jurisdiction in which the awarding body or centre are operating.

In JCQ's General Regulations for Approved Centres (section 6.1) reference is made to 'data protection legislation'. This is intended to refer to UK GDPR, the Data Protection Act 2018 and any statutory codes of practice issued by the Information Commissioner in relation to such legislation.

Pupils 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

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

Section 1 – Exams-related information

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 5 – Candidate information, audit and protection measures*.

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

- Awarding Bodies
- Joint Council for Qualifications
- Department for Education; Local Authority; Multi Academy Trust; Consortium; the Press;

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

- hard copy
- email
- secure extranet– AQA Centre Services; OCR Interchange; Pearson Edexcel Online; WJEC Secure services;

- a Management Information System (MIS) provided by Capita SIMS. Sending/receiving information via electronic data interchange (EDI) using A2C (https://www.jcq.org.uk/about-a2c) to/from Awarding Body processing systems.

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.

Section 2 – Informing candidates of the information held

St Richard's Catholic College ensures that candidates are fully aware of the information and data held.

All candidates are:

- informed via centre newsletter, electronic communication,
- given access to this policy via, centre website or written request.

Candidates are made aware of the above at the start of their course of study leading to 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 UK GDPR (or law relating to personal data in any jurisdiction in which the awarding body or centre are operating).

Candidates eligible for access arrangements which require Awarding Body approval using *Access Arrangements Online* are also required to provide their consent by signing the GDPR compliant JCQ candidate personal data consent form before approval applications can be processed online.

Section 3 – Hardware and software

The table below confirms how IT hardware, software and access to online systems is protected in line with DPA & GDPR requirements.

Hardware	Date of purchase and protection measures	Warranty expiry
Desktops	Various purchase dates, all within 4 years old. Systems report faults and errors centrally. Operating Systems are re-imaged termly. Snap shot backups are taken 3 times a day and held for 8 days. Data is replicated across two sites. Antivirus is updated daily	Various
Laptops	Various purchase dates, all within 4 years old. Systems report faults and errors centrally. Operating Systems are re-imaged termly. Snap shot backups are taken 3 times a day and held for 8 days. Data is replicated across two sites. Antivirus is updated daily	December 2023
Servers	Various purchase dates, all within 7 years old. Systems report faults and errors centrally. Operating Systems are re-imaged	November 2021

	termly. Snap shot backups are taken 3 times a day and held for 8 days. Data is replicated across two sites. Antivirus is updated daily	

Software/online system	Protection measure(s)
SIMS	SIMS server has restricted access, both physically and virtually. The database is backed up 3 times a day and held for 8 days. The data is replicated across two site as well as being held offsite.
Internet access	Internet access is filtered and restricted for all users. Access is defined by roles, with students receiving the highest level of restrictions and Exam users having zero access to the internet.
A2C	A2C is hosted on one of our servers, it is backed up 3 times a day and held for 8 days. The data is replicated across two sites. Access is restricted to IT Admins, SIMS Admin, Business Manager and the Exams Officer.

Section 4 – Dealing with data breaches

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
- cyber-attacks involving ransomware infections

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

1. **Containment and recovery**

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

2. **Assessment of ongoing risk**

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?

3. Notification of breach

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.

4. Evaluation and response

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

Section 5 – Candidate information, audit and protection measures

For the purposes of this policy, all candidates' exam-related information – even that not considered personal or sensitive under the DPA/GDPR – will be handled in line with DPA/GDPR guidelines.

An information audit is conducted yearly.

The table below details the type of candidate exams-related information held, and how it is managed, stored and protected

Protection measures may include:

- password protected area on the centre's intranet
- secure drive accessible only to selected staff
- information held in secure area
- updates are continuous and automatic (this may include updating antivirus software, firewalls, internet browsers etc.)

Section 6 – Data retention periods

Details of retention periods, the actions taken at the end of the retention period and method of disposal are contained in the centre's Exam's Archiving Policy which is available/accessible from the Centre Website or by written request.

Section 7 – Access to information

(with reference to ICO information https://ico.org.uk/your-data-matters/schools/exam-results/)

The GDPR gives individuals the right to see information held about them. This means individuals can request information about them and their exam performance, including:

- their mark
- comments written by the examiner
- minutes of any examination appeals panels

This does not however give individuals the right to copies of their answers to exam questions.

Requesting exam information

Requests for exam information can be made to Mrs Daniela Fletcher (Exams Officer), or Mr Mike Hollingsworth (Director of IT Services), in writing or email. If a former candidate is unknown to current staff identification will be required.

The GDPR does not specify an age when a child can request their exam results or request that they aren't published. When a child makes a request, those responsible for responding should take into account whether:

- the child wants their parent (or someone with parental responsibility for them) to be involved; and
- the child properly understands what is involved.

The ability of young people to understand and exercise their rights is likely to develop or become more sophisticated as they get older. As a general guide, a child of 12 or older is expected to be mature enough to understand the request they are making. A child may, of course, be mature enough at an earlier age or may lack sufficient maturity until a later age, and so requests should be considered on a case by case basis.

A decision will be made by Head of Centre as to whether the student is mature enough to understand the request they are making, with requests considered on a case by case basis.

Responding to requests

If a request is made for exam information before exam results have been published, a request will be responded to:

- within five months of the date of the request, or
- within 40 days from when the results are published (whichever is earlier).

If a request is made once exam results have been published, the individual will receive a response within one month of their request.

Third party access

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 Data Protection Officer will confirm the status of these agreements and approve/reject any requests.

Publishing exam results

When considering publishing exam results, St Richard's Catholic College will make reference to the ICO (Information Commissioner's Office) https://ico.org.uk/your-data-matters/schools/exam-results/ Can schools give my exam results to the media for publication?

Section 8 – Table recording candidate exams-related information held

For details of how to request access to information held, refer to section 7 of this policy (**Access to information**)

For further details of how long information is held, refer to section 6 of this policy (**Data retention periods**)

Information type	Information description (where required)	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 outcome(s) Specialist report(s) (may also include candidate address) Evidence of normal way of working	Access Arrangements Online MIS Filing system, with secure lockable room.	Secure user name and password In secure area solely assigned to SENCo	
Alternative site arrangements		Candidate Name Exam Number	Exams Office Secure Server	In Secure Room Password	
Attendance registers copies		Candidate name Exam Number	Exams Office	In Secure Room	Until after the deadline for EAR BTEC – 3 years
Candidates' work		Candidate name Exam Number	Exam Papers are dispatched the day of the exam. If this is not possible they are stored	In Secure Room or safe	Until after the deadline for EAR BTEC – 3 years

Information type	Information description (where required)	What personal/sensitive data is/may be contained in the information	Where information is stored	How information is protected	Retention period
			in the Examination Safe overnight. Coursework- Exam Safe or lockable storage facility within departments		
Candidate Scripts		Candidate Name Candidate Number	Exams Office With Subject Staff	Names and candidate numbers are removed from the scripts	3 years
Certificates		**Candidate Name** **Qualification and Result**	Exams Office	Secure Room	
Certificate destruction information	.	Candidate Name Qualifications Exam Number	Secure Room	Secure Room	1 year
Certificate issue information	Prize Giving Evening Collection in Person			Candidates identified by staff. ID required if not possible	
Conflicts of Interest records		Staff Name Candidate Names Subject Information	Exams Office Secure Server	Secure Room Secure Server	After EARs

Information type	Information description (where required)	What personal/sensitive data is/may be contained in the information	Where information is stored	How information is protected	Retention period
		Relationship			
Entry information		**Candidate Name** **Exam Number** **Subject information (including tier of entry where required)**	MIS	Password	
Exam room incident logs		Candidate Name Exam Number	Exams Office	Secure Room	Until after the EAR deadline
Invigilator and facilitator training records		Invigilator and Facilitator Names	Exams Office Secure Server	Secure Room Password	Until after the EAR deadline
Overnight supervision information		Candidate Name Exam Number Address Subject information	Exams Office Secure Server	Secure Room Password	Until after the EAR deadline
Post-results services: confirmation of candidate consent information		Candidate Name Exam Number Subject Information	Exams Office Secure Server	Secure Room Password	Until after the EAR deadline
Post-results services: requests/outcome information		Candidate Name Exam Number Subject Information Candidate Grades	Exam board secure sites MIS Secure Server	Password	Until after the EAR deadline

Information type	Information description (where required)	What personal/sensitive data is/may be contained in the information	Where information is stored	How information is protected	Retention period
Post-results services: scripts provided by ATS service		Candidate Name Exam Number Subject Information Marking	Exam board secure sites MIS Hard Copies in Department	Password The majority of copies are distributed electronically and are protected by the secure server. Any hard copies are locked within departments. Candidate names and numbers are removed.	
Post-results services: tracking logs		Candidate Name Exam Number Subject Information	All processed via Exam Boards Secure Sites	Password	
Private candidate information		Candidate Name Exam Number Subject Information	Exam board secure sites MIS Secure Server	Password	Until after the EAR deadline
Resolving clashes information		Candidate Name Exam Number Subject Information	MIS	Password	Until after the EAR deadline

Information type	Information description (where required)	What personal/sensitive data is/may be contained in the information	Where information is stored	How information is protected	Retention period
Results information		Candidate Name Exam Number Subject Information Grade	MIS	Password	
Seating plans		Candidate Name Exam Number	MIS Exams Office	Password Secure Room	
Special consideration information		Candidate Name Exam Number Reasons for Special Consideration	MIS Exams Office Exams Boards Secure Site	Password Secure Room	Until after the EAR deadline
Suspected malpractice reports/outcomes		Candidate Name Exam Number Circumstances of Malpractice	Exams Office Secure Server Exams Boards Secure Site	Secure Room Password Password	Until after the EAR deadline
Transferred candidate arrangements		Candidate Name Exam Number Course work	MIS Exams Office Exams Boards Secure Site	Password Secure Room	3 years

Information type	Information description (where required)	What personal/sensitive data is/may be contained in the information	Where information is stored	How information is protected	Retention period
		Subject Information Grades already received			
Very late arrival reports/outcomes		Candidate Name Exam Number Exam information Reason for late arrival	Exams Office Exams Boards Secure Site MIS	Secure Room Password	Until after the EAR deadline