



ST PETER'S CATHOLIC SCHOOL

Data Protection Policy (Exams)

Approved by FRP: November 2023
Ratified by Full Governing Body: December 2023

Due for review: October 2024

Public Sector Equality Duty. We have carefully considered and analysed the impact of this policy on equality and the possible implications for those with protected characteristics, as part of our commitment to meet the Public Sector Equality Duty (PSED) requirement to have due regard to the need to eliminate discrimination, advance equality of opportunity and foster good relations

Key staff involved in the policy

Role	Name(s)
Head of centre	Ben Doyle
Exams officer	Sandie Haskell
Senior leader(s)	RGD, BW, JWR, SP, NTR, RO, HPS
IT manager	Matt Slaughter
Data administer	Linda Hole

Purpose of the policy

This policy details how [insert centre name], 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).

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 these *General Regulations* 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. (JCQ [General Regulations for Approved Centres](#) (section 6.1) **Personal data**)

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

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 office(r) to hold exams-related information on candidates taking external examinations. For further details on the type of information held please refer to Section 5 below

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

- Awarding bodies
- Joint Council for Qualifications (JCQ)
- Department for Education
- Local Authority
- Press
- Social Media

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

- hard copy
- email
- secure extranet site(s)
 - eAQA
 - AQA Centre Services
 - OCR Interchange
 - Edexcel online
 - WJEC Secure site
- ESS SIMS

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 Peter’s School ensures that candidates are fully aware of the information and data held.

All candidates are:

- informed via St Peter’s School’s Data Protection Policy
- given access to this policy via centre website, written request.

Candidates are made aware of the above at the start of their 2-year examination courses.

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.

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
Laptop	June 2021 Encryption Anti-malware Offline back-up Internet filter – smoothwall	
Server	Physically locked in server room Anti-malware Off-line back-up	N/A

Software/online system	Protection measure(s)
ESS SIMS	Protected username/password Rules for password setting Password change every 6 months
Office	Protected username/password Rules for password setting Password change every 6 months Email back-up HR has to approve creation of new accounts IT support determine access rights
A2C	Password protected
TEAMS	Protected username/password Rules for password setting Password change every 6 months
4Matrix	Protected username/password Rules for password setting Password change every 6 months

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

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

1. Containment and recovery

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 every 2 years.

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 undertaken continually via online system

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 Exams archiving policy which is available/accessible from the Exam Manager

Section 7 – Access to information The GDPR gives individuals the right to see information held about them. This means individuals can request information about them and their exam results, 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 by email to data@st-peters.bournemouth.sch.uk, this must include a completed subject access request form which can be found on the school website under GDPR. Photographic ID will be required in the case of an ex-student. All subject assessed requests will be assessed individually.

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.

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 the Senior Information Risk Officer 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 results have been announced, 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 it has been authorised relative to the school’s 3rd party systems policy.

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.

Sharing information with parents

The centre will take into account any other legislation and guidance regarding sharing information with parents (including non-resident parents), as example guidance from the Department for Education (DfE) regarding parental responsibility and school reports on pupil performance:

- Understanding and dealing with issues relating to parental responsibility
www.gov.uk/government/publications/dealing-with-issues-relating-to-parental-responsibility/understanding-and-dealing-with-issues-relating-to-parental-responsibility
- School reports on pupil performance
www.gov.uk/guidance/school-reports-on-pupil-performance-guide-for-headteachers

Publishing exam results

St Peter's School will publish exam results to the media or within the centre (e.g. on an honours board) in line with the following principles:

- Refer to guidelines as published by the Joint Council for Qualifications
- Act fairly when publishing results, and where people have concerns about their or their child's information being published, taking those concerns seriously
- Ensure that all candidates and their parents/carers are aware as early as possible whether examinations results will be made public and how this will be done
- Explain how the information will be published. For example, if results will be listed alphabetically, or in grade order

As [insert centre name] will have a legitimate reason for publishing examination results, consent is not required from students or their parents or guardians for publication. However, if a student or their parents or guardians have a specific concern about publication of their results, they have the right to object. This objection must be made in writing to the Head of Centre or Deputy Head with responsibility for examinations, who will consider the objection before making a decision to publish and reply with a good reason to reject the objection to publish the exam results.

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 Lockable metal filing cabinet TEAMS	Secure user name and password In secure office (SENCo)	DOB of the pupil + 25 years
Alternative site arrangements	Exams to be taken at a venue other than school	Candidate Name Candidate #	Exam board secure site Exam laptop Hard copy	Secure user name and password In secure office	until the deadline for reviews of marking has passed or until any appeal, malpractice or other results enquiry has been completed, whichever is later
Attendance registers copies		Candidate Name Candidate #	Hard copy	In secure office	until the deadline for reviews of marking has passed or until any appeal, malpractice or other results enquiry has been completed, whichever is later
Centre consortium arrangements for centre assessed work	N/A	N/A	N/A	N/A	N/A

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
Certificates	Official Document	Candidate name Candidate DOB Exam Results	Hard copy of uncollected certificates	In secure office	2 years
Certificate destruction information	Information relating to destroyed uncollected certificates	Candidate name	Spreadsheet on exam laptop	Secure user name and password In secure office	4 years
Certificate issue information	A record of certificates that have been issued.	Candidate name	Printed lists	In secure office	4 years
Conflicts of Interest records	Staff declarations of conflict of interest with regards to exams	Staff names Candidate names	Exam laptop	Secure user name and password In secure office	until the deadline for reviews of marking has passed or until any appeal, malpractice or other results enquiry has been completed, whichever is later
Entry information		Candidate name Candidate DOB Gender	Exam board secure site Exam laptop Hard copy	Secure user name and password In secure office	until the deadline for reviews of marking has passed or until any appeal, malpractice or other results enquiry has been completed, whichever is later

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
Exam room incident logs	Record of any incidents arising during an examination	Candidate Name Log of incident details	Hard copy	In secure office	until the deadline for reviews of marking has passed or until any appeal, malpractice or other results enquiry has been completed, whichever is later
Invigilator and facilitator training records		Invigilator Names	Hard Copy Online training on The Exam Office	Secure user name and password In secure office	until the deadline for reviews of marking has passed or until any appeal, malpractice or other results enquiry has been completed, whichever is later
Overnight supervision information		Candidate Name Candidate #	Hard Copy Online training on The Exam Office	Secure user name and password In secure office	until the deadline for reviews of marking has passed or until any appeal, malpractice or other results enquiry has been completed, whichever is later
Post-results services: confirmation of candidate consent information		Candidate Name Candidate # Email address Home address	Hard copy Exam Boards websites	Secure user name and password In secure office	until the deadline for reviews of marking has passed or until any appeal, malpractice or other results enquiry has been completed, whichever is later

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: requests/outcome information		Candidate Name Candidate # Email address	Hard copy Exam Boards websites email	Secure user name and password In secure office	until the deadline for reviews of marking has passed or until any appeal, malpractice or other results enquiry has been completed, whichever is later
Post-results services: scripts provided by ATS service		Candidate Name Candidate # Exam answers	Exam board secure website Exam laptop	Secure user name and password In secure office If used in class – name redacted	until the deadline for reviews of marking has passed or until any appeal, malpractice or other results enquiry has been completed, whichever is later
Post-results services: tracking logs		Candidate Name Candidate # Results	Spreadsheet	Secure user name and password In secure office	until the deadline for reviews of marking has passed or until any appeal, malpractice or other results enquiry has been completed, whichever is later
Private candidate information		Candidate Name Candidate # Email address Home address	Email Exam Laptop	Secure user name and password In secure office	until the deadline for reviews of marking has passed or until any appeal, malpractice or other results enquiry has been completed, whichever is later

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
Resolving timetable clashes information		Candidate Name Candidate #	Email Exam Laptop Hard copy MIS	Secure user name and password In secure office	until the deadline for reviews of marking has passed or until any appeal, malpractice or other results enquiry has been completed, whichever is later
Results information		Candidate Name Candidate # Results	Exam Laptop Hard copy MIS	Secure user name and password In secure office at the start of their 2 year examination courses	Current year + 6 years
Seating plans		Candidate Name Candidate #	Hard copy MIS	Secure user name and password In secure office	until the deadline for reviews of marking has passed or until any appeal, malpractice or other results enquiry has been completed, whichever is later
Special consideration information		Candidate Name Candidate # Reason for consideration	Hard copy Exam Board website	Secure user name and password In secure office	until the deadline for reviews of marking has passed or until any appeal, malpractice or other results enquiry has been completed, whichever is later
Suspected malpractice reports/outcomes		Candidate Name Candidate # Details of Malpractice	Exam board secure website Exam laptop Hard copy	Secure user name and password In secure office	until the deadline for reviews of marking has passed or until any appeal, malpractice or other results enquiry has been completed, whichever is later

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
Transferred candidate arrangements		Candidate Name Candidate # Candidate exam entries	Exam board secure website Exam laptop	Secure user name and password In secure office	until the deadline for reviews of marking has passed or until any appeal, malpractice or other results enquiry has been completed, whichever is later
Very late arrival reports/outcomes	Details of candidates who arrive after the exam secure perios	Candidate Name Candidate # Reasons for late arrival	Hard copy Exam board secure website	Secure user name and password In secure office	until the deadline for reviews of marking has passed or until any appeal, malpractice or other results enquiry has been completed, whichever is later