Data Protection Policy (Exams)

2026/27

This policy is reviewed annually to ensure compliance with current regulations

Approved/reviewed by	
Adam Palmer	
Date of next review	September 2027

Key staff involved in the policy

Role	Name(s)
Head of centre	**Adam Palmer**
Exams and Data Officer	**Jocelyn Watson**
Senior leader(s)	**Lou Baker, Hannah Austin, Roisin Still, Simon Ralph, Rob Rooney**
IT manager	**IT St Thomas Catholic Trust**
Data manager	**DPO- Maxine Gilmartin**
Data Officer	**Hayley Boswell**

Purpose of the policy

This policy details how St Michael's Catholic School 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).

As an all-through school, this policy only applies to exams taken on the Secondary phase.

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) **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 and Data Manager 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 of Education
- Buckinghamshire County Council
- Other schools on transfer at Post-16
- Secure web applications (e.g. SISRA) to facilitate school performance management

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

- hard copy
- email
- secure extranet site(s) – AQA Centre Services; OCR Interchange; Pearson Edexcel Online; WJEC Secure Website, London Institute of Banking and Finance (LiBF), Princes Trust, Trinity Arts Award
- 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
- Secure website (s) – Sisra Analytics, ALPS, FFT

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 Michael's Catholic School ensures that candidates are fully aware of the information and data held.

All candidates are:

- informed via the privacy policy issued with the data forms given to all new students
- given access to this policy via hard copy when they are admitted to the centre and a copy is also available on the school website.

Candidates are made aware of the above when a candidate starts at secondary school (any year group)

At the start of each academic year, 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). This is sent out to electronically to parents and pupils in Years 10 – 13 (or individually to anyone in the lower year groups if they are taking a public exam.

Candidates eligible for access arrangements which require awarding body approval 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 and GDPR requirements.

Hardware		Date of purchase and protection measures	Warranty expiry
Desktop computers Laptops		Desktop computers used for exams are in Classroom 1/17 1/18,1/19. 1/10 and 1/09 and are approximately 8 yrs old. Hardware is checked on a weekly basis by the on-site IT Team and always checked for functionality prior to planned exams. All hard-drives are encrypted. Classrooms are locked after use. Anti-virus software is provided by Sophos and continually updated on the Main Server and replicated out to any devices on the school's Domain. The Sophos Dashboard on the Server is checked on a	The desktop warranty has expired. All issues are fixed by on-site IT Team.

		daily basis for any anomalies. Laptops are managed by the Exams & Data Officer and kept in a secure environment. Sophos is automatically downloaded to the Laptop when it is logged into the school's Domain.	

Software/online system	Protection measure(s)
SIMS, OneDrive, Teams, Word, Excel	All Apps and Programs are accessed via/or stored on, the school Network which is protected by Sophos (as stated above). New Network accounts are authorised by the Exams & Data Officer. School Network usernames and passwords are managed by the on-site IT Team and issued on an individual basis. [The current password processes are being revised, to ensure they meet *DfE Information and Communication Technologies Security Policy* regulations]. Once logged on to a PC/Laptop, to access any Apps and Programs, each user will have a further individual logon and password, managed by the App or Program owner. O365/Teams usernames and passwords are managed by the on-site IT Team and issued on an individual basis. [The current password processes are being revised, to ensure they meet *DfE Information and Communication Technologies Security Policy* regulations]. SIMS usernames and passwords and are managed by IT support
St Michael's Main Server	Main Server logon details are stored in a passworded secure area on the external IT Consultants web portal. No access is given to any personnel outside of the on-site IT Team. Network Usernames and Passwords are managed by the on-site IT Team and are held on Active Directory on the school's Main Server. Access can only be made by the on-site IT Administrators.

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 or Business Manager 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?

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.

3. **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.

The table in Section 8 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
- Anti-virus software is provided by Sophos and continually updated on the Main Server and replicated out to any devices on the school's Domain. The Sophos Dashboard on the Server is checked on a daily basis for any anomalies

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 Teacher's network drive

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 the Exams and Data Officer using the school Request for Information form (available on the school website) or via email to exams@stmichaelscs.org

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 the Exams and Data Manager and/or a member of SLT 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.

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

Section 8 – Table recording candidate exams-related information held

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's with agreed access arrangements in place	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 Network drive	Secure user name and password In secure office (SENCo) Secure user name and password	Until the candidate is 25 years old
Attendance registers copies	Those attending the exams for each subject	Candidate Name Candidate Exam Number	MIS Secure storage room	Secure user name and password Secure key holder access only	6 months after the end date to request a Review of Results
Candidates' scripts	Answer booklets/WP scripts	Candidate Name Candidate Exam Number	Secure storage facility	Key holder access	Until dispatched to awarding body
Candidates' work	NEA/Coursework	Candidate Name Candidate Exam Number	MIS or network drives Head of Department Classrooms	Secure user name and password Keys only held by staff	6 months after the end date to request a Review of Results

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	Grades achieved for each subject	Candidate Name Candidate Exam Number Candidate ULN Grades achieved	Reception for first 4 months after receipt Secure room 5 – 12 months after receipt	Locked cupboard Key holder access only	12 months from date of issue
Certificate destruction information	Certificates not collected by candidates	Candidate Name Subject and Grades achieved Series date	Network drive - spreadsheet	Secure user name and password	4 years after destruction
Certificate issue information	Collectors name and date of collection of certificates	Candidate Name Candidate Exam Number Candidate ULN Grades achieved Name of person collecting	Paper lists in Reception for first 4 months after receipt Secure room 5 – 12 months after receipt Written permission forms in EM's office	Locked cupboard Key holder access only Restricted access to office	3 years
Conflicts of interest records	Name of staff member	Staff name Name/details	Paper copy in EM's office	Restricted access to office	6 months after the end date to request a Review of Results
Entry information	Candidates entered for subjects	Candidate Name Candidate Exam Number Candidate ULN	MIS Paper copies signed off by HOD in EM's office	Secure user name and password Restricted access to office	6 months after the end date to request a Review of Results

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	Incidents occurring in the exam room	Candidate Name Candidate Exam Number Details of incident	Paper logs in secure room	Key holder access only	6 months after the end date to request a Review of Results
Invigilator and facilitator training records		Staff name	Network drive Paper copies in exams office	Secure user name and password Restricted access to office	12 months
Overnight supervision information	N/A				
Post-results services: confirmation of candidate consent information	Requests for RoR	Candidate Name Candidate Exam Number Candidate Email Candidate Phone Number	Network drive Paper copies in exams office	Secure user name and password Restricted access to office	6 months after the end date to request a Review of Results
Post-results services: requests/outcome information	Awarding body letters	Candidate Name Candidate Exam Number Grade information	Network drive Paper copies in exams office	Secure user name and password Restricted access to office	6 months after the end date to request a Review of Results
Post-results services: scripts provided by ATS service	Candidate scripts	Candidate Name Candidate Exam Number Marks Achieved	Network drive Email	Secure user name and password Secure user name and password	6 months after the end date to request a Review of Results

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: tracking logs	Candidate Requests	Candidate Name Candidate Exam Number	Network drive Paper copies in exams office	Secure user name and password Restricted access to office	6 months after the end date to request a Review of Results
Private candidate information	Candidates entered for subjects	Candidate Name Candidate Exam Number Candidate Email Candidate Phone Number	Network drive Paper copies in exams office	Secure user name and password Restricted access to office	6 months after the end date to request a Review of Results
Resolving timetable clashes information	Candidates entered for subjects	Candidate Name Candidate Exam Number	Network drive Paper copies in exams office	Secure user name and password Restricted access to office	6 months after the end date to request a Review of Results
Results information	Candidates entered for subjects	Candidate Name Candidate Exam Number Grade information	MIS Paper copies in exams office or secure room	Secure user name and password Restricted access to office	Ongoing 6 months after the end date to request a Review of Results
Seating plans	Candidates entered for subjects	Candidate Name Candidate Exam Number Access arrangements in place	MIS Paper copies in exams office or secure room	Secure user name and password Restricted access to office	Ongoing 6 months after the end date to request 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
					Review of Results
Special consideration information	Candidates entered for subjects	Candidate name Candidate DOB Candidate exam number Medical reports including from consultants/GPs/CAMHs Other documents/emails	Network drive Paper copies in exams office	Secure user name and password Restricted access to office	6 months after the end date to request a Review of Results
Suspected malpractice reports/outcomes	Candidate reported for suspected malpractice	Candidate name Candidate exam number Staff names – invigilator, HOC etc	Network drive Paper copies in exams office	Secure user name and password Restricted access to office	6 months after the end date to request a Review of Results
Transferred candidate arrangements	Candidate information	Candidate name Candidate exam number	MIS/JCQ CAP Email	Secure user name and password	Ongoing
Very late arrival reports/outcomes	Candidate information	Candidate name Candidate exam number Parental information	MIS/JCQ CAP Email Paper copies in exams office	Secure user name and password Restricted access to office	Ongoing 6 months after the end date to request a Review of Results