St Matthew Academy

GENERAL DATA PROTECTION REGULATION (EXAMS)

Policy

Our motto is 'Let your light shine'. It is taken from St Matthew's Gospel and captures our belief in the uniqueness of each individual. Our aim is to ensure that the talents and strengths of each pupil are encouraged, developed and celebrated.

Successful, confident learners

High expectations, outstanding achievements

Inclusive, caring, Catholic community

Nurturing talent, cultivating ambition

Excellence for all

Date of Approval	**Autumn 2019**
Review Date	**Autumn 2020**

Key staff involved in the policy

Role	Name(s)
Head of centre	**Ms M Baldwin**
Exams officer	**Ms F Walker**
Exams officer line manager (Senior leader)	**Ms S Wickliffe**
IT manager	**RM Unify**
Data manager	**Ms B Crammond**

Purpose of the policy

This policy details how St Matthew Academy, 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.

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 – Candidate information, audit and protection measures.

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

- Awarding bodies
- Joint Council for Qualifications (JCQ)
- Local Authority
- Department for Education
- Law enforcement bodies and government bodies (where legally obliged to do so)
- Alternative centre if the candidate is being transferred

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

- hard copy
- email
- secure extranet site(s) – eAQA; OCR Interchange; Pearson Edexcel Online; WJEC Secure services; City & Guilds Walled Garden; RSL; NCFE
- 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.

Informing candidates of the information held

St Matthew Academy ensures that candidates are fully aware of the information and data held.

All candidates are:

- informed via examinations booklet
- given access to this policy via the centre website

Candidates are made aware of the above prior to entry for external examinations. 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.

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	Protection measures	Warranty expiry
• Desktop Computer • Laptop	All St Matthew Academy computers and laptops require users to enter their user name and an 8 digit password	N/A

Software/online system	Protection measure(s)
Capita SIMS	All users must enter an individual ID and password Access rights are controlled by the Data Manager
Awarding Body Secure Sites: • Edexcel Online • eAQA • WJEC Secure Site • OCR Interchange • RSL • NCFE	Access to the secure sites is password protected Access rights and accounts are controlled by the Exams Officer
A2C	Accounts are limited to Data Manager and Exams Officer

	Access is via Secure Key issued by awarding body

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:

Containment and recovery

Business manager, currently Paul Lawson, 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

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.

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

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 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 regularly (this may include updating antivirus software, firewalls, internet browsers etc.)

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 Examinations Officer and on the Academy website.

Access to information

Current and former candidates can request access to the information/data held on them by making a subject access request to the Business manager in writing by letter or email. If former candidate is not known to any current member of staff, photo ID will be required. All requests will be dealt with within 40 calendar days.

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

Personal data about a candidate belongs to that candidate, and not the candidate's parents or carers. For a parent or carer to make a subject access request with respect to their child, the candidate must either be unable to understand their rights and the implications of a subject access request, or have given their consent.

Children aged 12 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils in secondary may not be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis

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

When considering publishing exam results, the centre will make reference to the ICO (Information Commissioner's Office) Education and Families https://ico.org.uk/for-organisations/education/ information on publishing exam results.

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	Secure user name and password In secure office (SENCo Office)	
Alternative site arrangements	Where a candidate is being transferred	Candidate name Candidate DOB Gender UCI	MIS Awarding body secure site	Secure user name & password	
Attendance registers copies		Candidate name Candidate DOB Gender	Locked office Secure Room	Locked office (Data & Exams Office) – entry via keycode Secure Room	
Candidates' scripts		Candidate name Candidate DOB UCI	Secure Storage Facility	Access limited to keyholders only	
Candidates' work					

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
Centre consortium arrangements for centre assessed work					
Certificates		Candidate Name	Lockable Cabinet	In locked office (Data & Exams Office)	Two years
Certificate destruction information		Candidate Name	Lockable Cabinet	In locked office (Data & Exams Office)	
Certificate issue information		Candidate Name & DoB	File held by Exams Officer	In locked office (Data & Exams Office)	
Conflicts of Interest records		Candidate Name & DoB	File held by Exams Officer	In locked office (Data & Exams Office)	
Entry information		Candidate Name, DoB, UCI	File held by Exams Officer SIMS	In locked office (Data & Exams Office) Password protected	
Exam room incident logs		Candidate Name & DoB	File held by Exams Officer	In locked office (Data & Exams Office) Secure Room	
Invigilator and facilitator training records		Invigilator Name	File held by Exams Officer	In locked office (Data & Exams Office)	
Overnight supervision information					
Post-results services: confirmation of candidate consent information		Candidate Name & DoB	File held by Exams Officer	In locked office (Data & Exams Office) Secure Room	

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 & DoB	File held by Exams Officer Exams Officer N: drive	In locked office (Data & Exams Office), Secure Room Access to drives via login	
Post-results services: scripts provided by ATS service					
Post-results services: tracking logs		Candidate Name, candidate number	Exams Officer N: drive		
Private candidate information	N/A	N/A	N/A	N/A	N/A
Resolving timetable clashes information					
Results information		Candidate Name, DoB & results	MIS – SIMS T: Drive SISRA Locked cabinet	MIS & SISRA are password protected T:drive folder access is limited to relevant staff only In locked office (Data & Exams Office)	
Seating plans		Candidate Name & Candidate Number	File held by Exams Officer	In locked office (Data & Exams Office) Secure Room	
Special consideration information		Candidate Name & DoB	File held by Exams Officer	In locked office (Data & Exams Office) Secure Room	

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
Suspected malpractice reports/outcomes		Candidate Name, Candidate Number & DoB	File held by Exams Officer	In locked office (Data & Exams Office) Secure Room	
Transferred candidate arrangements	Transferred candidate arrangements	Candidate Name & DoB	File held by Exams Officer	In locked office (Data & Exams Office) Secure Room	
Very late arrival reports/outcomes	Very late arrival reports/outcomes	Candidate Name, Candidate Number & DoB	File held by Exams Officer	In locked office (Data & Exams Office) Secure Room	