General Data Protection Regulation (GDPR) policy - Exams

Magna Academy

Approved by Regional Board:		**Date:** September 2020
Last reviewed on:	September 2020	
Next review due by:	September 2021	

Key staff involved in the General Data Protection Regulation policy

Role	Name(s)
Head of centre	**Ms Natasha Ullah**
Exams officer	**Mrs Arlene Ellaway**
Exams officer line manager (Senior Leader)	**Mr Adam Potter**
Data Protection Officer	**Ms Jennifer Morrison**
IT manager	**Mr Adrian Patterson**
Data manager	**Ms Angela Jones**

Purpose of the policy

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

At the date of reviewing these regulations, although the UK has left the European Union the General Data Protection Regulation still has a direct effect within the UK (JCQ's General Regulations for Approved Centres (GR, 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
- not transferred outside the European Economic Area without adequate protection

To ensure that the centre meets the requirements of the DPA and 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 – 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 site(s) –eAQA; OCR Interchange; Pearson Edexcel Online; WJEC Secure services
- Management Information System (MIS) provided by Advanced (Progresso) 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

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

All candidates are:

- informed via electronic communication
- given access to this policy via centre website and/or written request

Candidates are made aware of the above at the start of their course of study leading to external examinations.

Section 3 – Hardware and software

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

Hardware	Date of purchase and protection measures	Warranty expiry

Software/online system	Protection measure(s)
MS Word 2016	Individual documents are created by students that contain the answers to the exam papers they sit on that day & time. This may contain their Candidate number and Centre number. The documents are backed up onto the Exam server and once printed and handed in to the invigilator at the end of the exam currently being sat, they are deleted from the network.

Pearson POP	The Pearson system is client/server based. All student/candidate data is entered via orders/bookings within the Pearson website and securely transferred to the server at Magna Academy. Students are then able to log-in with IDs generated by the Pearson software, take the test online and submit the results. Pearson are ultimately in control of the delivery, storage and retention of any data containing Candidate numbers etc.
Access to Computer Systems and Email	The Magna network requires enforced password changes every 90 days for staff and 360 days for students. Passwords must be complex – contain a combination of letters and non-alphabetic characters and be a minimum of 8 characters in length. Email is provided via a cloud based system (Office 365) which makes it more difficult for a virus to send automated emails from the Magna network. All web traffic is monitored and filtered.

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**

IT Manager & 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 annually

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 every 6 months (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 Exams archiving policy available/accessible from The Exams Officer.

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 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

Current and former candidates can request access to the information/data held on them by making a **subject access request** to the Data Protection Officer in writing. Former candidate unknown to current staff will need to provide an exam result slip/certificates with photographic ID. All requests will be dealt with within 40 calendar days.

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 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 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, except in section 1, 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

Magna Academy 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

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)	Access arrangements online In secure area solely accessed to by exams/SEND department	Password protected In secure area solely accessed to by exams/SENDCo	3 years
Attendance registers copies		n/a	Exam office		6 months
Candidates' work	Coursework		Secure storage in curriculum areas		After EAR
Certificates		Name/DOB Student signature of receipt	Exam store	In secure area solely assigned to exams	10 years
Certificate destruction information	.	Candidate name	Exam store	In secure area solely assigned to exams	Indefinitely
Certificate issue information		Candidate name	Exam store	In secure area solely assigned to exams	Indefinitely

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
Entry information		Name/DOB	Exam office MIS	In secure area solely assigned to exams Password protected	6 months
Exam room incident logs		Candidate name	Exam office	In secure area solely assigned to exams	After EAR
Overnight supervision information		Name/DOB/Address/signature	Exam office	In secure area solely assigned to exams	After EAR
Post-results services: confirmation of candidate consent information		Name/signature	Exam office	In secure area solely assigned to exams	9 months
Post-results services: requests/outcome information			Exam office MIS	In secure area solely assigned to exams Password Protected	9 months
Post-results services: scripts provided by ATS service			Exam office		9 months
Post-results services: tracking logs			Exam office	In secure area solely assigned to exams	9 months
Private candidate information		Name/DOB/Address/photo ID Proof of ID	Exam office MIS	In secure area solely assigned to exams Password protected	9 months
Resolving clashes information		n/a	Exam office	In secure area solely assigned to exams	After EAR
Results information		Name/DOB Signature of receipt	Exam office MIS	In secure area solely assigned to exams Password protected	5 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
Seating plans		n/a	Exam office	In secure area solely assigned to exams	6 months
Special consideration information		Name/DOB/sensitive information	Exam store	In secure area solely assigned to exams	6 months
Suspected malpractice reports/outcomes		Candidate name/DOB	Exam office	In secure area solely assigned to exams	9 months
Transferred candidate information		Name/DOB/address	Exam office	In secure area solely assigned to exams	6 months
Very late arrival reports/outcomes		Candidate name	Exam office	In secure area solely assigned to exams	6 months