

Maplewell Hall School



Exams General Data Protection Regulation Policy (adopted from Exams Office template)

Policy Created	March 2019
Annual review by	Exams Officer
Last review	Autumn 2024
Amendments required	Autumn 2024
Approved by head of centre	Autumn 2024

Contents

1. Purpose of the policy	3
2. Exams-related information.....	3
3. Informing candidates of the information held	4
4. Hardware and software	5
5. Dealing with data breaches	6
Containment and recovery.....	6
Assessment of ongoing risk.....	7
Notification of breach.....	7
Evaluation and response	7
6. Candidate information, audit and protection measures	7
7. Data retention periods	8
8. Access to information	8
Requesting exam information	8
Responding to requests.....	9
Third party access	9
Sharing information with parents	9
9. Table recording student exams-related information held	10

1. Purpose of the policy

This policy details how Maplewell Hall 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).

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.

It is the responsibility of the centre to inform candidates of the processing that the centre undertakes. For example, that the centre will provide relevant personal data including name, date of birth, gender to the awarding bodies for the purpose of examining and awarding qualifications.

All exams office staff responsible for collecting and sharing students' 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.

2. Exams-related information

There is a requirement for the exams office(r) to hold exams-related information on students 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

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

- hard copy
- email
- secure extranet site(s) – e.g. AQA centre services; OCR Interchange, Pearson Edexcel Online, WJEC Secure services, Gateway, City & Guilds Walled Garden; Duke of Edinburgh, Sports Leaders, Access Arrangements Online
- 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; etc.

This data may relate to exam entries, access arrangements, the conduct of exams and non-examination assessments including controlled assessments and coursework, special consideration requests and exam results/post-results/certificate information.

3. Informing candidates of the information held

Maplewell Hall School ensures that candidates are fully aware of the information and data held.

All students are:

- informed via electronic communication
- given access to this policy via centre website

Candidates are made aware of the above at the start of their course, or when the registration/entries are submitted to awarding bodies for processing.

Materials which are submitted by candidates for assessment may include any form of written work, audio and visual materials, computer programmes and data (“Student Materials”). Candidates will be directed to the relevant awarding body’s privacy notice if they require further information about how their Student Materials may be used by the awarding body.

Candidates eligible for access arrangements/reasonable adjustments 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.

4. 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
Desktop	Purchase Date: N/A. Exam logins created by IT department. Internet and spellcheck removed. Stored and locked in exam room.	N/A
Laptop	Purchase Date: N/A. Exam logins created by IT department. Internet and spellcheck removed. Stored and locked in exam room.	N/A
Reading Pens	Purchase Date: November 2018. Exam Reading pens are removed from classrooms ensuring that anything stored in the internal storage is removed.	N/A

Software/online system	Protection measure(s)
SIMS	Protected usernames and passwords for all staff members. Centre administrator has to approve the creation of new user account and determine access rights. Staff deleted when they are no longer employed. Regular checks to Firewall/Antivirus software.
Go4Schools	Protected usernames and passwords for all staff members. Centre administrator has to approve the creation of new user account and determine access rights. Staff deleted when they are no longer employed. Regular checks to Firewall/Antivirus software.

WEDUC	Protected usernames and passwords for all staff members. Centre administrator has to approve the creation of new user account and determine access rights. Staff deleted when they are no longer employed. Regular checks to Firewall/Antivirus software.
Awarding Body Websites	Only authorised staff to be given logins by the Exams Officer. Staff deleted when they are no longer employed. Regular checks to Firewall/Antivirus software.
A2C	Only installed onto one computer (the Exams Officer). Regular checks to Firewall/Antivirus software.

5. 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:

Containment and recovery

- County Council 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

6. Candidate information, audit and protection measures

For the purposes of this policy, all students' 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 student exams-related information held, and how it is managed, stored and protected.

Protection measures include:

- Password protected area on the centre's intranet
- Secure drive accessible only to selected staff
- Information held in secure area
- Updates undertaken every month (this may include updating antivirus software, firewalls, internet browsers etc.)

7. 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 exams officer upon request.

8. 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

Current and former students can request access to the information/data held on them by making a **subject access request** to County Hall in writing. 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.

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 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 and a local authority (the 'corporate parent'), 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
(Updated 24 August 2023 to include guidance on the role of the 'corporate parent', releasing GCSE results to a parent and notifying separated parents about a child moving school)
- **School reports on pupil performance**
www.gov.uk/guidance/school-reports-on-pupil-performance-guide-for-headteachers

9. Table recording student 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	What personal/sensitive data is/may be contained in the information	Where information is stored	How information is protected	Retention period
Access arrangements information	Student Name Date of Birth Gender Data protection notice (student signature) Diagnostic testing outcome(s) Specialist report(s) (may also include student address) Evidence of normal way of working	Access arrangements online MIS Password protected spreadsheet Lockable filing cabinet	Secure user name and password In secure area solely assigned to exams	Until student is 30 years old
Attendance registers copies	Student Name Exam Number	MIS Lockable filing cabinet	In secure area solely assigned to exams	1 year
Students' work	Student Name Exam Number	Lockable filing cabinet/room	In secure area solely assigned to exams	1 year
Certificates	Student Name ULN	Shared Drive with limited access MIS Lockable filing cabinet	Secure user name and password In secure area solely assigned to exams	12 months from date of issue

Information type	What personal/sensitive data is/may be contained in the information	Where information is stored	How information is protected	Retention period
Certificate destruction information	Student Name	Shared Drive with limited access Lockable filing cabinet	In secure area solely assigned to exams	4 years from date of destruction
Certificate issue information	Student Name Correspondence Address	Shared Drive with limited access Lockable filing cabinet	In secure area solely assigned to exams	4 years from the date of issue
Entry information	Student Name Date of Birth Gender Exam Number ULN UCI	Shared Drive with limited access MIS Exam Board Website Lockable filing cabinet	Secure user name and password In secure area solely assigned to exams	1 year
Exam room incident logs	Student Name	Lockable filing cabinet	In secure area solely assigned to exams	1 year
Overnight supervision information	Student Name Exam Number	Lockable filing cabinet	In secure area solely assigned to exams	1 year
Post-results services: confirmation of student consent information	Student Name Date of Birth Exam Number	Shared Drive with limited access Exam Board Websites Lockable filing cabinet	Secure user name and password In secure area solely assigned to exams	1 year

Information type	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	Student Name Date of Birth Exam Number	Shared Drive with limited access Exam Board Websites Lockable filing cabinet	Secure user name and password In secure area solely assigned to exams	1 year
Post-results services: scripts provided by ATS service	Student Name Date of Birth Exam Number	Shared Drive with limited access Exam Board Websites Lockable filing cabinet	Secure user name and password In secure area solely assigned to exams	1 year
Post-results services: tracking logs	Student Name Date of Birth Exam Number	Shared Drive with limited access Exam Board Websites Lockable filing cabinet	Secure user name and password In secure area solely assigned to exams	1 year
Private student information	Name Date of Birth Gender Correspondence Address Phone Number	Shared Drive with limited access MIS Exam Board Website Lockable filing cabinet	Secure user name and password In secure area solely assigned to exams	1 year
Resolving clashes information	N/A	N/A	N/A	N/A

Information type	What personal/sensitive data is/may be contained in the information	Where information is stored	How information is protected	Retention period
Results information	Student Name Date of Birth Gender Exam Number ULN UCI	Shared Drive with limited access MIS Exam Board Website Lockable filing cabinet	Secure user name and password In secure area solely assigned to exams	1 year
Seating plans	Student Name Exam Number	MIS Lockable filing cabinet	Secure user name and password In secure area solely assigned to exams	1 year
Special consideration information	Student Name Date of Birth Gender Exam Number ULN UCI	Shared Drive with limited access MIS Exam Board Website Lockable filing cabinet	Secure user name and password In secure area solely assigned to exams	1 year
Suspected malpractice reports/outcomes	Student Name Date of Birth Gender Exam Number	Shared Drive with limited access MIS Exam Board Website	Secure user name and password In secure area solely assigned to exams	1 year

Information type	What personal/sensitive data is/may be contained in the information	Where information is stored	How information is protected	Retention period
	ULN UCI	Lockable filing cabinet		
Transfer of credit information	Student Name Date of Birth Gender Exam Number ULN UCI	Shared Drive with limited access MIS Exam Board Website Lockable filing cabinet	Secure user name and password In secure area solely assigned to exams	1 year
Transferred student information	Student Name Date of Birth Gender Exam Number ULN UCI	Shared Drive with limited access MIS Exam Board Website Lockable filing cabinet	Secure user name and password In secure area solely assigned to exams	1 year
Very late arrival reports/outcomes	Student Name Date of Birth Gender Exam Number ULN	Shared Drive with limited access MIS Exam Board Website Lockable filing cabinet	Secure user name and password In secure area solely assigned to exams	1 year

Information type	What personal/sensitive data is/may be contained in the information	Where information is stored	How information is protected	Retention period
	UCI			