



Monkton Wood Academy

DATA PROTECTION POLICY

(Exams)

2025/26

This policy is reviewed annually to ensure compliance with current regulations

Approved/reviewed by	
Date of next review	November 2026

Key staff involved in the policy

Role	Name(s)
Head of centre	Hannah Jones
Exams officer	Laura Moore
Senior leader(s)	Louise Husband
IT manager	Alan Higginson
Data manager	Jackie Baddoo

Contents

Key staff involved in the policy	2
Purpose of the policy	4
Section 1 – Exams-related information	4
Section 2 – Informing candidates of the information held	5
Section 3 – Hardware and software	5
Section 4 – Dealing with data breaches.....	6
Section 5 – Candidate information, audit and protection measures	7
Section 6 – Data retention periods.....	7
Section 7 – Access to information	7
Section 8 – Table recording candidate exams-related information held	10

Purpose of the policy

This policy details how Monkton Wood 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 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) 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 and gender to the awarding bodies for the purpose of examining and awarding qualifications.

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
- Cabot Learning Federation (CLF) - Multi-Academy Trust

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; Cambridge OCR Interchange; Pearson Edexcel Online; WJEC Portal; etc.
- Management Information System (MIS) provided by Bromcom 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 including controlled assessments and coursework, special consideration requests and exam results/post-results/certificate information.

Section 2 – Informing candidates of the information held

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

All candidates are:

- informed via candidate handbook
- given access to this policy via academy website.

Candidates are made aware of the above during GCSE qualifications or when the registrations/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 programs 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 will be informed that an application for access arrangements will be processed using *Access arrangements online*, complying with the UK GDPR and the Data Protection Act 2018.

Candidates involved in suspected or alleged malpractice will be informed that their personal data will be provided to the awarding body (or bodies) whose examinations/assessments are involved, and that personal data about them may also be shared with other awarding bodies, the qualifications regulator or professional bodies, in accordance with the JCQ document *Suspected Malpractice – Policies and Procedures*.

Candidates will be informed:

- that awarding bodies may be required to provide a candidate's personal data to educational agencies, such as DfE, Welsh Government, Department of Education (Northern Ireland), ESFA, regulators, HESA, UCAS, Local Authorities and the Learning Records Service (LRS)
- that their personal data may be provided to a central record of qualifications approved by the awarding bodies for statistical and policy development purposes
- of the processing that the centre undertakes, for example, that the centre will provide relevant personal data, including name, date of birth and gender, to the awarding bodies for the purpose of examining and awarding qualifications

Candidates may obtain access to their personal data, such as examination results by applying to the appropriate awarding body's data protection officer.

Candidates are also referred to the centre's privacy notice which explains:

- why Monkton Wood Academy needs to collect personal data
- what it plans to do with it
- how long it will keep it
- whether it will be sharing it with any other organisation

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
Desktop and laptop computers	PCs and laptops are regularly cloned from updated MS Windows images, hardware state is checked and all data on local hard drives is wiped during this operation. Computers on school network are protected by firewall and antivirus is installed on all computers and set up to actively	Manufacturer's warranty until expired

	scan files on access. Anti-malware is installed on all computers and scheduled to run regular scans	
Software/online system	Protection measure(s)	
Bromcom	Protected usernames and passwords; rules for password setting (use of a mix of upper/lower cases letters and numbers) Password changes Data Manager creates user accounts and determines access rights Uses Single Sign On (SSO) through Office 365	
Awarding Bodies Secure extranet sites	Protected usernames and passwords; rules for password setting (use of a mix of upper/lower cases letters and numbers) Password changes Exams Officer creates user accounts and determines access rights Two-step Authenticator Login	
Office 365 One Drive	Two-step Authenticator Login Protected usernames and passwords; rules for password setting (use of a mix of upper/lower cases letters and numbers) Password changes	

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

Operations manager or data manager will lead on investigating the breach (supported by CLF security officer).

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 can be conducted by operations manager or CLF centralised teams.

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 in accordance with centralised CLF IT Team processes (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 which is available/accessible from: *in 'MWA All Staff' – policies'*.

Section 7 – Access to information

(With reference to ICO information <https://ico.org.uk/for-the-public/schools/exam-results/>)

The UK 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 exams@mwa.clf.uk

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 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 (Last 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

Publishing exam results

When considering publishing exam results, Monkton Wood Academy will make reference to the ICO (Information Commissioner's Office) <https://ico.org.uk/for-the-public/schools/exam-results/> Can schools give my exam results to the media for publication?

OR

Monkton Wood Academy 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 Monkton Wood Academy will have a legitimate reason for publishing examination results, consent is not required from students or their parents/carers for publication. However, if a student or their parents/carers have a specific concern about publication of their results, they have the right to object. This objection must be made in writing to exams@mwa.ccf.uk, 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 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	MFA; Secure username and password In secure office	
Alternative site arrangements					
Attendance registers copies		Candidate name Candidate number	In box file Locked within the secure office	In secure office	
Candidates' scripts		Candidate name Candidate number Candidate signature	In secure access area within the secure office	Locked secure access area with metal shutters No outside window	
Candidates' work					
Centre consortium arrangements for centre assessed work					
Certificates		Candidate name	Lockable metal filing cabinet	In secure office	

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
		Candidate DOB Candidate results			
Certificate destruction information		Candidate name Candidate number	Lockable metal filing cabinet	In secure office	
Certificate issue information		Candidate name Candidate signature	Lockable metal filing cabinet	In secure office	
Conflicts of interest records		Name	In folder locked within the secure office	In secure office	
Entry information		Candidate name Candidate number	MIS	Secure username and password	
Exam room incident logs		Candidate name Candidate number	Locked within the secure office	In secure office	
Invigilator and facilitator training records		Invigilator/ Facilitator names	In folder locked within the secure office	In secure office	
Overnight supervision information					
Post-results services: confirmation of candidate consent information		Candidate name Candidate number Candidate signature Candidate personal email address	Post-results services spreadsheet tracker Forms in folder locked within the secure office	Secure username and password Secure drive In secure office	
Post-results services: requests/outcome information		Candidate name Candidate number Candidate result	Post-results services spreadsheet tracker	Secure username and password Secure drive	

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: scripts provided by ATS service		Candidate name Candidate number Candidate signature	Secure drive	Secure username and password Secure drive	
Post-results services: tracking logs		Candidate name Candidate number Candidate result	Post results services spreadsheet tracker	Secure username and password Secure drive	
Private candidate information					
Resolving timetable clashes information		Candidate name Candidate number	MIS	Secure username and password	
Resilience arrangements: Evidence of candidate performance					
Results information		Candidate name Candidate DOB UCI and ULN numbers Candidate result	MIS	Secure username and password	
Seating plans		Candidate name Candidate number	MIS In folder locked within the secure office	Secure username and password In secure office	
Special consideration information		Candidate name Candidate number Candidate address Candidate DOB	On spreadsheet tracker and folder	Secure username and password In secure office	

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
		Personal email address			
Suspected malpractice reports/outcomes		Candidate name Candidate number	Secure drive In folder locked within the secure office	Secure username and password In secure office	
Transferred candidate arrangements					
Very late arrival reports/outcomes					