HASMONEAN MULTI ACADEMY TRUST

Data Protection Policy (Exams)

2023/24

This policy is reviewed annually to ensure compliance with current regulations

Approved/reviewed by	
J Leigh/L Oskis	
Date of next review	Autumn 2024

Key staff involved in the policy

Role	Name(s)
Heads of centre	**M Langdon/K Brice**
Exams officers	**J Leigh/ J Owusu**
Exams officer line manager (Senior leader)	**L Oskis**
IT manager	**O Smirnov**
Data manager	**Y Oskis**
Centre Administrator	**L Finkelstein**
DPO	**A Harris Ellis**

Purpose of the policy

This policy details how Hasmonean Multi-Academy Trust in relation to exams management and administration, ensures compliance with the regulations as set out by the Data Protection Act 2018 (DPA 2018) and the 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.

Students have 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 who are 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 Officers 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) – e.g. eAQA; Pearson Edexcel Online; WJEC Secure services
- The 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; the LRS

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

Hasmonean MAT ensures that candidates are fully aware of the information and data held.

All candidates are:

- informed via assemblies/email/ information on the school website
- given access to this policy following a written request

Candidates are made aware of the above at the start of their course of study, and that this will lead to an externally accredited qualification.

At this point, the centre also brings to the attention of the 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.

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 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 & GDPR requirements.

Hardware	Date of purchase and protection measures	Warranty expiry
Desktop and lap top 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 provided by London Grid for Learning Sophos antivirus is installed on all computers and set up to actively scan files on access Malwarebytes anti-malware is installed on all computers and scheduled to run regular scans.	Manufacturer's warranty until expired

Software/online system	Protection measure(s)
Bromcom MIS	Bromcom is a cloud based MIS so all its data is hosted by Bromcom Computers Plc. Reference should be made to the GDPR Compliance and privacy statement https://www.bromcom.com/Resources/Misc/GDPR.pdf
eAQA	Usernames are selected by administrator and checked for uniqueness by AQA. Passwords and password recovery question are also selected by administrator. Password must be between 6 and 16 characters. It must include either 2 numbers (0-9) and 4 letters (a-z, A-Z) or 4 numbers (0-9) and 2 letters (a-z, A-Z). It is case sensitive and no requirement to change password regularly. Centre administrator has to approve the creation of new user accounts and determine access rights.

Edexcelonline	Username must be your e-mail address EdexcelOnline. Passwords are case sensitive, they must be between 8-15 characters in length and should be alphanumeric. Passwords should contain at least one uppercase letter and should not contain username, first name or last name. Passwords should not contain any spaces or special characters other than @ _ - . They are e-mailed direct to user No requirement to change password regularly Centre administrator has to approve the creation of new user accounts and determine access rights;
WJEC	User account is centre number for administrator and centre number followed by 3 letters for others. Passwords must be at least 8 characters and contain at least one letter and one number. Must not include " @*;?! No requirement to change password regularly Centre administrator has to approve the creation of new user accounts and determine access rights;
A2C	Software is downloadable but to use one needs an access key and password for each board which can only be obtained from the examination board.
LRS	Username based on first part of surname and chosen by site. Password must be at least 8 characters long and must be made up of at least three of the following four character types: An upper case letter; A lower case letter; A number; A special character. Password must be changed every three months. User account is managed by LRS not by user
Cambridge Assessment Extranet	Username is e-mail address Password must be at least 6 characters long, containing at least two numbers. No requirement to change password regularly. User account is managed by Cambridge Assessment

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, Mrs Harris-Ellis, 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 every autumn.

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 areas
- updates undertaken - most of the updates run automatically whenever the computers are online, PCs and laptops. Those include windows updates, browsers, antivirus and antimalware updates. Updates of the school's networking equipment (switches, access points) are triggered manually when new firmware version become available. Other networking devices (firewalls and routers) are provided and maintained by London Grid for Learning and also updated regularly.

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 from the Exams Officers on request.

Section 7 – Access to information

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.

(with reference to ICO information https://ico.org.uk/your-data-matters/schools/exam-results/)

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/email. Any former candidate unknown to staff will need to attend the school with photographic ID before a request can be dealt with. All candidates should make an appointment with the relevant member of staff. All requests will be dealt with within one month.

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 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 exam results have been published, a request will be responded to:

- within five months of the date of the request, or
- within 30 days from when the results are published (whichever is earlier).

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, such as a parent or carer, unless a request is accompanied with permission from the candidate and appropriate evidence (where relevant), to verify the ID of both parties has been 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
- 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, Hasmonean MAT will make reference to the ICO (Information Commissioner's Office) https://ico.org.uk/your-data-matters/schools/exam-results/ Can schools give my exam results to the media for publication?

Publishing examination results is a common and accepted practice. Many students enjoy seeing their name in print, particularly in the local press and GDPR does not stop this happening. However, under GDPR schools have to act fairly when publishing results, and where people have concerns about their or their child's information being published, schools must take those concerns seriously.

Schools should make sure that all pupils and their parents or guardians are aware as early as possible whether examinations results will be made public and how this will be done. Schools should also explain how the information will be published. For example, if results will be listed alphabetically, or in grade order.

In general, because a school has a legitimate reason for publishing examination results, pupils or their parents/carers do not need to give their consent to publication. However, if you have a specific concern about publication of your results, you have the right to object. Schools should consider objections from pupils and parents/carers before making a decision to publish. A school would need to have a good reason to reject someone's objection to publication of their 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 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 (SENDCo)	
Alternative site arrangements		N/a			
Attendance registers copies		Details of candidates' names, exam nos, access arrangements	In a file in the secure storage	Locked room only accessible by 5 key holders	6 months
Candidates' scripts		Details of candidates' names, exam nos	In a lockable cabinet in the secure storage	Locked room only accessible by 5 key holders	24 hours maximum
Candidates' work		Details of candidates' names, exam nos	In a lockable cabinet in the secure storage	Locked room only accessible by 5 key holders	3 years maximum
Centre consortium arrangements for centre assessed work		Details of candidates' names, exam nos	On staff computer	Secure user name and password	1 year maximum

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		Details of candidates' names, exam nos and results	In the lockable exam office in a filing cabinet	In the lockable exam office in a filing cabinet	Minimum 12 months
Certificate destruction information		Details of candidates' names, exam nos and results	On desktop computer, if relevant	Secure user name and password. Lockable office	7 years minimum
Certificate issue information		Details of candidates' names, exam nos and results	In the lockable exam office in files ranked A-Z	In the lockable exam office	Minimum 12 months
Conflicts of Interest records	Details of members of staff who are taking exams / preparing their children for exams	Details of candidates' names, exam nos, entries	Exam boards sites/ email/ staff computer	Secure user name and password	Minimum 12 months
Entry information		Details of candidates' names, exam nos, entries	Bromcom MIS. Folder in exams office	Secure user name and password. Lockable office.	Minimum 12 months
Exam room incident logs		Details of candidates' names, exam nos, entries, medical conditions	In a file in the secure storage	Locked room only accessible by 4 key holders	6 months
Invigilator and facilitator training records		Names and signatures	In the lockable exam office in an invigilator file	In the lockable exam office	12 months
Overnight supervision information		Details of candidates' names, exam nos, entries. Parents' details.	In the lockable exam office in a file	In the lockable exam office	6 months
Post-results services: confirmation of candidate consent information		Details of candidates' names, contact details, exam nos, entries,	In the lockable exam office in a file	In the lockable exam office	6 months

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		Details of candidates' names, contact details, exam nos, entries, results	In the lockable exam office in a file	In the lockable exam office	6 months
Post-results services: scripts provided by ATS service		Details of candidates' names, contact details, exam nos, entries, results	In a lockable cabinet in the secure storage	Given to staff immediately. Staff reminded to shred scripts confidentially	6 months
Post-results services: tracking logs		Details of candidates' names, contact details, exam nos, entries, results	Spreadsheet on staff desktop computer	Secure user name and password. Lockable exam office	6 months
Private candidate information		Entries, results, access arrangements, medical conditions, contact information	Bromcom MIS. Folder in exams office	Secure user name and password. Lockable exam office	12 months
Resolving timetable clashes information		Details of candidates' names, exam nos, entries, access arrangements	Bromcom MIS. Spreadsheet on staff computer	Secure user name and password. Lockable exam office	12 months
Results information		Candidate entries and results	Bromcom MIS. Spreadsheet on staff computer	Secure user name and password. Lockable exam office	12 months mimimum
Seating plans		Details of candidates' names, exam nos, entries, access arrangements	In the secure storage in a file	Locked room only accessible by 4 key holders	6 months
Special consideration information		Details of candidates' names, exam nos, entries, access arrangements, medical / personal information	Spreadsheet on staff computer. Folder in the lockable exam office	Secure user name and password. Lockable exam office	12 months

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		Details of candidates' names, exam nos, entries, details of suspected malpractice	Folder in the lockable exam office. Exam Board websites	Secure user name and password. Lockable exam office	12 months
Transferred candidate arrangements	Transferred candidate arrangements	Details of candidates' names, exam nos, entries	Folder in the lockable exam office. Exam Board websites	Secure user name and password. Lockable exam office	12 months
Very late arrival reports/outcomes	Very late arrival reports/outcomes	Details of candidates' names, exam nos, entries. Personal/ medical information relevant to the late arrival	Folder in the lockable exam office. Exam Board websites	Secure user name and password. Lockable exam office	6 months