Data Protection policy (exams)

2021-2022

Approved by	
The Governing Body approved this statutory policy	
Date of next review	October 2022

Key staff involved in the General Data Protection Regulation policy

Role	Name(s)
Head of centre	**Tony Roe**
Exams officer	**Laura Bradford Dawn Hosier**
Exams officer line manager (Senior Leader)	**Pete Flaxman**
Data Protection Officer	**Yvonne Mason**
IT manager	**Paul Leake**
Data manager	**Elaine Webster**

Purpose of the policy

This policy details how Barking Abbey School, in relation to exams management and administration, ensures compliance with the regulations as set out by the Data Protection Act (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 these *General Regulations* 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. (JCQ General Regulations for Approved Centres (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

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 below*

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

- Awarding bodies
- Joint Council for Qualifications
- Department for Education; Local Authority; the Press

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

- hard copy
- email
- secure extranet site(s) – eAQA; AQA Centre Services; OCR Interchange; Pearson Edexcel Online; WJEC Secure services
- Management Information System (MIS) provided by Capita SIMS sending/receiving information via electronic data interchange (EDI) using A2 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

Barking Abbey School 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

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

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.

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 computers x 3	01/07/2016 Security updates – monthly	3 years

	AV updates - daily AV Scans - daily	
Server Storage	31/03/2013 Multiple redundant backups Redundant components for failover Power failure protection Security updates – monthly or as need for zero-day issues AV Updates – daily ISP Firewall protection Stored in a temperature-controlled room, with intruder alarm and fire alarm protection	Ongoing – renewed yearly

Software/online system	Protection measure(s)
MIS - SIMS.Net	Security controlled by permissions in SIMS, only authorised user granted access to exams data. SIMS logon linked to computer network logon, passwords are force change every three months and complex passwords must be used.
A2C	Install restricted to one exam officer computer and one exam officer logon only. Password only known to exam officer and is a complex password.

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**

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 yearly.

Commented [LP1]: Initially only one has been done for GDPR

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
- security updates are undertaken every month
- Antivirus updates are undertaken daily

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 the Exams office and centre website.

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

Requests for exam information can be made to the Data Protection Officer in writing or by email.

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 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.

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	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 area solely assigned to exams SENCo secure filing	4 years after candidate has left the centre
Attendance registers copies	Candidate name Invigilator signature	Exams Office	Secure room	To be retained until after the deadline for EARs or until any appeal, malpractice or other results enquiry has been completed, whichever is later.
Candidates' work	Candidate name Candidate signature Marks awarded	HOD secure storage prior to dispatch Exams Office once returned	Secure room	To be retained until after the deadline for EARs or until any appeal, malpractice or other results enquiry has been completed, whichever is later. Returned to candidate or destroyed as appropriate
Certificates	Candidate name Candidate DOB Candidate grades	Exams Office Lockable metal filing cabinet	Secure room	5 years
Certificate destruction information	Candidate name Candidate DOB	Exams Office Lockable metal filing cabinet	Secure room	5 years after confidential destruction

Information type	What personal/sensitive data is/may be contained in the information	Where information is stored	How information is protected	Retention period
	Candidate grades			
Certificate issue information	Candidate name Candidate DOB Candidate grades	Exams Office Lockable metal filing cabinet	Secure room	5 years
Conflict of Interest	Candidate name Staff name	Electronically	Secure user name and password	to be retained until after the deadline for EARs or until any appeal, malpractice or other results enquiry has been completed, whichever is later.
Entry information	Candidate name Candidate DOB ULN,UCI	Exams Office Lockable filing cabinet MIS	Secure Room Secure user name and password	Hard copies to be retained until after the deadline for EARs or until any appeal, malpractice or other results enquiry has been completed, whichever is later. MIS information: Student date of Birth plus 25 years
Exam room incident logs	Candidate name	Exams Office	Secure room	To be retained until after the deadline for EARs or until any appeal, malpractice or other results enquiry has been completed, whichever is later.
Overnight supervision information	Candidate name	Exams Office	Secure room	To be retained until after the deadline for EARs or until any appeal, malpractice or other results enquiry has been completed, whichever is later.
Post-results services: confirmation of candidate consent information	Candidate name Candidate signature	Exams Office	Secure room	To be retained until after the deadline for EARs or until any appeal, malpractice or other results enquiry has been completed, whichever is later.
Post-results services: requests/outcome information	Candidate name Candidate grades	Exams Office AB secure website	Secure room	To be retained until after the deadline for EARs or until any appeal, malpractice or other results enquiry has been completed, whichever is later.

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: scripts provided by ATS service	Candidate name Candidate question responses	Exams Office Electronic copies	Secure room Secure user name and password accessed staff drive	To be retained until after the deadline for EARs or until any appeal, malpractice or other results enquiry has been completed, whichever is later.
Post-results services: tracking logs	Candidate name	Exams Office	Secure room	To be retained until after the deadline for EARs or until any appeal, malpractice or other results enquiry has been completed, whichever is later.
Private candidate information	Candidate name Candidate DOB Candidate Address Candidate contact details; email, phone Copy of photographic ID	Exams Office MIS	Secure room Secure user name and password	To be retained until after the deadline for EARs or until any appeal, malpractice or other results enquiry has been completed, whichever is later. MIS: Student date of Birth plus 25 years
Resolving clashes information	Candidate name	Exams Office	Secure room	To be retained until after the deadline for EARs or until any appeal, malpractice or other results enquiry has been completed, whichever is later.
Results information	Candidate name Candidate grades	Exams Office MIS SISRA	Secure room Secure user name and password	MIS: Student date of Birth plus 25 years
Seating plans	Candidate name Invigilator signature	Exams Office MIS	Secure room Secure user name and password	To be retained until after the deadline for EARs or until any appeal, malpractice or other results enquiry has been completed, whichever is later.
Special consideration information	Candidate name Candidate DOB	Exams Office AB secure website	Secure room Secure user name and password	To be retained until after the deadline for EARs or until any appeal, malpractice or other results enquiry has been completed, whichever is later.

Information type	What personal/sensitive data is/may be contained in the information	Where information is stored	How information is protected	Retention period
	Candidate address: GP or other professional evidence letter Details of any relevant medical condition, Police enquiry, death certificate			
Suspected malpractice reports/outcomes	Candidate name Candidate grade	Exams Office	Secure room	To be retained until after the deadline for EARs or until any appeal, malpractice or other results enquiry has been completed, whichever is later.
Transferred candidate information	Candidate name	Exams Office	Secure room	To be retained until after the deadline for EARs or until any appeal, malpractice or other results enquiry has been completed, whichever is later.
Very late arrival reports/outcomes	Candidate name	Exams Office	Secure room	To be retained until after the deadline for EARs or until any appeal, malpractice or other results enquiry has been completed, whichever is later.