



The Bishop of Hereford's Bluecoat School

Exam Data Protection Draft Policy

SLT Lead: Ellie Bunston

Governor Committee Approval: AQT

Review Date: September 2026

Key staff involved in the policy

Role	Name(s)
Head of centre	Tom Williams
Exams officer	Clara Lobban
Senior leader(s)	Ellie Bunston
IT manager	Sean Mason
Data manager	Joe Christopher

Purpose of the policy

This policy details how Bishop of Hereford Bluecoat 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 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 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)

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 Website;

- 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;
- 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

The Bishop of Hereford Bluecoat School ensures that candidates are fully aware of the information and data held.

All candidates are:

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

Candidates are made aware of the above at the start of a course leading to a vocational qualification, or, where candidates are following GCE and GCSE qualifications, when the entries are submitted to awarding bodies for processing.

At this point, the centre also brings to the attention of 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 (or law relating to personal data in any jurisdiction in which the awarding body or centre are operating).

1. Candidates eligible for access arrangements which require awarding body approval 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 computer Laptop/tablet	Hardware checked by Sean Mason Anti-Virus up to date	N/A

Software/online system	Protection measure(s)
MIS SIMS	Password protected
Awarding body secure extranet site(s)	Password protected

--	--

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

Joe Christopher 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?

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 regularly.

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 in line with guidelines for example: Anti-virus is updated everyday with a new virus signature Automatically, Windows updates are pushed out roughly every month via IT or sooner depending on the security risk/awareness, Other application depends on when an update is available (Chrome will update itself. IE/Edge is included as part of windows Updates as and when) Firewalls are updated by our ISP 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 [insert e.g. Exams Archiving Policy] which is 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 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 the exams officer in writing.

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 the Deputy Headteacher 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.

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**)

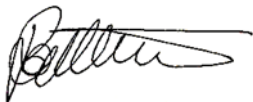
Information type	Information description (where required)	What personal/sensitive data is/may be contained in the information	Where information is stored	How information is protected	Retention period
Access arrangements information		Candidate name Candidate DOB Gender Data protection notice (candidate 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 [insert] In secure office (SENCo)	
Alternative site arrangements		N/A			
Attendance registers copies		Cand name and number	In locked exams cupboard		
Candidates' scripts		Cand name and number	In secure office		
Candidates' work		Cand name and number	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
Centre consortium arrangements for centre assessed work		N/A			
Certificates		Cand name and number	In secure office		
Certificate destruction information		Cand name/results	In locked exams office		
Certificate issue information		Cand signature	In locked exams office		
Conflicts of interest records		Staff signature	With exams officer		
Entry information		Cand name Gender	On MIS system		
Exam room incident logs		Cand name and number	In locked exams office		
Invigilator and facilitator training records		Name of invigilator	Online in MIS system or exams office online records (password protected)		

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
Overnight supervision information		N/A			
Post-results services: confirmation of candidate consent information			In locked exams office		
Post-results services: requests/outcome information			In locked exams office		
Post-results services: scripts provided by ATS service			In locked exams office		
Post-results services: tracking logs			In locked exams office		
Private candidate information			N/A		
Resolving timetable clashes information			N/A		
Results information		Cand name, number, results	In secure server area		

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		Cand name and number	In locked exams office and MIS password protected areas		
Special consideration information		Cand name number details of incident	In locked exams office		
Suspected malpractice reports/outcomes		Cand name number details of incident	In locked exams office		
Transferred candidate arrangements			N/A		
Very late arrival reports/outcomes		Cand name number details of incident	In locked exams office		

Approved by the AQT Governors Committee at their meeting of the 6th November 2025

A handwritten signature in black ink, appearing to be 'P. Allen', written in a cursive style.

Signed:

(Chair of AQT Governors Committee)