



Data Protection Policy (Exams) 2025-26	Revision No	2
	Date Issued	April 2026
	Authorised by	Chair of Governors
	Date approved	19 April 2026
	Minute number	EA 19/04/2026
	Implementation Date	20 April 2026
	Review Date	March 2027

Contents

Purpose, Values and Aims of Highfields School	2
1. Key staff involved in the policy	3
2. Purpose of the policy	3
3. Exams-related information.....	4
4. Informing candidates of the information held.....	4
5. Hardware and software	5
6. Dealing with data breaches	6
7. Candidate information, audit and protection measures.....	8
8. Data retention periods.....	9
9. Access to information	9

Purpose, Values and Aims of Highfields School

Our Core Purpose

To be an inclusive, happy community that values every individual and inspires them to achieve their full potential.

Our Values

Inclusion, fairness and equality

Respect and tolerance

Celebration of achievement

Personal reflection, honesty and mutual trust

Care for our environment

Aims – to achieve our core purpose and values we aim to:

- Respect all students and staff as individuals
- Celebrate diversity and promote equality
- Provide appropriate levels of challenge
- Develop understanding and enjoyment of learning
- Support and encourage individuals to make a valuable contribution to society
- Be a reflective school seeking continuous improvement
- Play an active part in our community
- Nurture physical and emotional well being
- Promote a happy, safe and stable environment

1. Key staff involved in the policy

Role	Name(s)
Head of centre	Andrew Marsh
Senior leader(s)	Peter Cole – Deputy Headteacher with oversight of examination administration
Exams Officer	Natasha Hubbard
IT Manager	Tom Cauldwell
Data/Exams Manager	Lizzy Dence

2. Purpose of the policy

This policy details how Highfields 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) 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.

3. Exams-related information

There is a requirement for the exams office 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
- Local Authority
- EMET (Multi Academy Trust)

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

- hard copy
- email
- secure extranet sites – AQA Centre Services; Cambridge OCR Interchange; Pearson Edexcel Online; WJEC Portal
- Management Information System (MIS) provided by Arbor
- 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.

4. Informing candidates of the information held

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

All candidates are:

- informed via electronic communication – privacy notice issued via Show My Homework and on the school website
- given access to this policy via the school website

Candidates are made aware of the above 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 Highfields School 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

5. 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
PCs / Laptops	Impero monitoring system in place; Sophos antivirus updates automatically; regular checks conducted by IT manager including hard drive scans and system integrity assessments. Many system scans are automated through Group Policy Object (GPO).	All devices have 5-year warranty.

Software/online system	Protection measure(s)
MIS (Arbor)	Protected usernames and passwords linked to secure school network access, rules for password setting, rules for regularity of password changing
Internet browsers	Regular checks to Firewall/Antivirus software
Documents in OneDrive	Protected usernames and passwords linked to secure school network access, rules for password setting, rules for regularity of password changing, two-factor authentication (2FA)
Awarding body secure extranet sites (AQA, OCR, Pearson Edexcel), WJEC Eduqas)	Two-factor authentication (2FA), centre administrator has to approve the creation of new user accounts and determine access rights
A2C	Secure access keys obtainable only by approved Exams Officer users of the awarding body secure extranet sites

6. 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 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

7. 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 annually.

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 every month on average (this may include updating antivirus software, firewalls, internet browsers etc.)

Candidate Information	Management/Storage	Protection
Candidate name, DOB, exam registration numbers etc.	MIS (Arbor), internal documents, awarding body secure extranet sites	Protected usernames and passwords linked to secure school network access, awarding body sites are protected by two-factor authentication and restricted to approved users
Centre assessed marks	Internal documents, input into awarding body secure extranet sites	Secure drive accessible only to selected staff, awarding body sites are protected by two-factor authentication and restricted to approved users
Access arrangement information	Internal documents, Provision Map software, JCQ AAO Portal	Secure drive accessible only to selected staff, Provision Map and JCQ AAO Portal are securely password protected, Regular checks to Firewall/Antivirus software
Exam results	MIS (Arbor), internal documents, awarding body secure extranet sites	Protected usernames and passwords linked to secure school network access, awarding body sites are protected by two-factor authentication and restricted to approved users
Special consideration information	Internal documents, awarding body secure extranet sites	Secure drive accessible only to selected staff, awarding body sites are protected by two-factor

		authentication and restricted to approved users, any hard copy evidence received is scanned then securely shredded
--	--	--

8. 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 in hard copy in the Exams Office, or via Every.

9. 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 the Exams Officer in writing. If a former candidate is unknown to current staff, their identity will need to be confirmed by providing a copy of their passport or driving licence.

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 Data Protection Officer 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'), for 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

Publishing exam results

When considering publishing exam results, Highfields School 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?