



Hyde High School

Exams Data Protection Policy

Date to be reviewed:	Autumn 2026
-----------------------------	--------------------

Key staff involved in the General Data Protection Regulation Policy

Role	Name(s)
Head of centre	Mr G Arnold
Exams Officer	Mr J Marsden
Exams officer line manager (Senior Leader)	Mrs L Poole
Data Manager	Mr M Brooks

Purpose of the Policy

This policy details how Hyde High School, in relation to exams management and administration, ensures compliance with the regulations as set out by the Data Protection Act (DPA) and the UK General Data Protection Regulation.

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
- not transferred outside the European Economic Area without adequate protection

To ensure that the centre meets the requirements of the DPA 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 officer 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 (password protected)
- Joint Council for Qualifications (password protected)
- Department for Education (password protected)
- Local Authority (password protected)
- Post-16 education and training providers (password protected)
- The local press/media.

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

- hard copy

- email ((password protected)
- secure extranet sites – eAQA; OCR Interchange; Pearson Edexcel Online; WJEC Secure services, BCS ECDL online and NCFE portal which only the exams officer and designated members of staff may use with secure, unique usernames and passwords.
- SIMS (a Management Information System (MIS) provided by Capita and Tameside Council SIMS team used for sending/receiving information via electronic data interchange (EDI) using A2C (<https://www.jcq.org.uk/about-a2c>) to/from awarding body processing systems. This is only used with secure, unique usernames and passwords.

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

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

All candidates are:

- Informed via the whole year assembly and school email.
- Given access to this policy via the school website.

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

Section 3 – Software

The table below confirms how IT software and access to online systems is protected in line with DPA & UK GDPR requirements.

Software/online system	Protection measure(s)
A2C Software	Provided by JCQ Each awarding body is API key protected Access to system is password protected
SIMS - Exams Organiser	Password protected
Exam Board Websites	Provided by the exam board. Password protected users and 2FA
Exams Assist (School Work Space)	Password protected
G4Schools	Password protected

Section 4 – Dealing with data breaches

Although data is handled in line with DPA/UK 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

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.

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/UK GDPR – will be handled in line with DPA/UK GDPR guidelines.

The Data Protection Officer will conduct an information audit 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 a secure area.
- Updates undertaken frequently (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 table below.

Section 7 – Access to 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 – valid ID will be requested if a former candidate is unknown to current staff. All requests will be dealt with within 40 calendar days.

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.

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 record/history and evidence and approval to support any application that has been made for exams.	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 SENCO office Secured shared staff folder	Secure username and password protected. Restricted access to school drive Restricted access to the office.	SEN records are kept 25 years from students' date of birth i.e. 9 years after leaving in year 11, after which they are disposed of in the red confidential waste bin. MIS ongoing.
Attendance registers copies	Copies of registers for all internal/external examinations	Candidate name and candidate number. Exam and tier of entry	In the Exams Officer office. MIS Exams Officers personal computer drive	In the Exams Officer office only accessed by regulated biometric access. All software is only accessed by a unique username and password held by Exams Officer.	Disposed of in red confidential waste bin after the EAR period or any appeals have ended, or within 12 months of any internal exams. MIS ongoing.
Candidates' work	Hard copies/Electronic copies of candidates' work	Candidate name and candidate number	In teachers' secure storage area or pupil folders on shared drive.	Pupil only access via password log-ins. IT and selected staff will have 'read only' access.	Until the deadline for EAR period or any appeals have ended.

Certificates	Formal certificates received from relevant boards	Candidate name Candidate DOB Subjects' results	In lockable cabinet with Exams Officer	Lockable unit until collected by student. Photo ID is used. Full records are kept of distribution of certificates.	At least 12 months after the candidate has left.
Entry information	Entry mark sheets and signed statement of entries	Candidate name and candidate number	Paper format in Exams Officer office MIS	Exams Officer office only accessed by regulated biometric access. All software only accessed by unique username and password held by Exams Officer.	Paper copies are disposed of in red confidential waste bin after the EAR period or any appeals have ended, or within 12 months of any internal exams. MIS ongoing.
Exam room incident logs	Log sheets for any issues during exams.	Candidate name and candidate number and incident information	Paper format in Exams Officer office	Exams Officer office only accessed by regulated biometric access.	Disposed of in red confidential waste bin after the EAR period or any appeals have ended.
Post-results services	Confirmation of candidate consent information Requests/outcome information Scripts provided by ATS service	Candidate name and candidate number Subject/tier of entry Service requested Signed consent form Outcome	Paper format in Exams Officer office Exams Officers personal computer drive	Exams Officer office only accessed by regulated biometric access.	Disposed of in red confidential waste bin after the EAR period or any appeals have ended.
Results information	Candidates results	Candidate name Candidate DOB Subjects' results	MIS	Restricted access to teaching staff.	Paper documentation disposed of securely after

					deadline for all EAR's. MIS ongoing.
Seating plans	Signed seating arrangements for all exams	Candidate name and candidate number Subject/tier Access arrangements	Paper format in Exams Officer office MIS	Exams Officer office only accessed by regulated biometric access.	Paper documentation disposed of securely after deadline for all EAR's. MIS ongoing..
Special consideration information	JCQ forms and relevant information for applying for special consideration for candidates	Candidate name and candidate number Subject/tier Any relevant proof Details of application	Exams Officers personal computer drive Paper format in Exams Officer office	Exams Officer office only accessed by regulated biometric access. All software is only accessed by a unique username and password held by Exams Officer.	Paper copies are disposed of in red confidential waste bin after the EAR period or any appeals have ended, or within 12 months of any internal exams.
Suspected malpractice reports/outcomes	JCQ forms and relevant information for any malpractice reports	Candidate name and candidate number Subject/tier Any relevant proof Details of application	Exams Officers personal computer drive Paper format in Exams Officer office	Exams Officer office only accessed by regulated biometric access. All software is only accessed by a unique username and password held by Exams Officer.	Paper copies are disposed of in red confidential waste bin after the EAR period or any appeals have ended, or within 12 months of any internal exams.

Transferred candidate information	JCQ forms	Candidate name and candidate number Subject/tier Access arrangements	Paper format in Exams Officer office MIS	Exams Officer office only accessed by regulated biometric access.	Paper documentation disposed of securely after deadline for all EAR's. MIS ongoing.
Very late arrival reports/outcomes	JCQ forms	Candidate name and candidate number Subject/tier Access arrangements	Paper format in Exams Officer office MIS	Exams Officer office only accessed by regulated biometric access.	Paper documentation disposed of securely after deadline for all EAR's. MIS ongoing.