



DISCOVERY
EDUCATIONAL TRUST

Data Protection Policy (Examinations) 2024/25

Title	Data Protection Policy (Examinations) 2024/25
Author/Owner	CHS and SMS Examinations Officers
Status	Final
Issue Date	Dec-24
Senior Leadership Team Review by	CHS - Colin Brodigan - Deputy Headteacher - Examinations and Timetable SMS - John Peacock - Assistant Headteacher - Assessment, Recording and Reporting
Review Cycle	Annual
Review Date	Sep-25
Security Classification	OFFICIAL

Contents

1. Purpose.....	3
2. Examinations-Related Information	3
3. Informing Candidates of the Information Held	4
4. Hardware and Software	4
5. Dealing with Data Breaches	4
Containment and Recovery	5
Assessment of Ongoing Risk	5
Notification of Breach	5
Evaluation and Response	6
6. Candidate Information, Audit and Protection Measures.....	6
7. Data Retention Periods	6
8. Access to Information	6
Requesting Exam Information	6
Responding to Requests	7
Third Party Access	7
Sharing Information with Parents/Carers.....	7
Publishing Examination Results	8
9. Table Recording Candidate Examinations-Related Information Held	9

1. Purpose

This Policy details how Chase High School (CHS) and St. Martin's School (SMS), in relation to the management and administration of examinations and assessments, ensure compliance with the regulations as set out by the Data Protection Act 2018 (DPA 2018) and UK General Data Protection Regulation (UK GDPR).

The delivery of examinations and assessments involves 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 Centres and Awarding Bodies comply with the requirements of the DPA 2018 and UK GDPR, or law relating to personal data in any jurisdiction in which the Awarding Body or Centre is 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 the DPA 2018 and UK GDPR, and any statutory codes of practice issued by the Information Commissioner in relation to such legislation.

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 Examinations Office staff, responsible for collecting and sharing candidates' data, are required to follow strict rules called 'data protection principles' ensuring that 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;
- retained for no longer than is absolutely necessary;
- handled in accordance with 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' examination information – even that which is not classified as personal or sensitive – is covered under this Policy.

2. Examinations-Related Information

There is a requirement for the Examinations Office(r) to hold examinations-related information on candidates taking external examinations. For further details on the type of information held, refer to Section 5 below.

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

- Awarding Bodies;
- Joint Council for Qualifications (JCQ);
- Department for Education (DfE);
- Local Authority (LA);
- The Multi Academy Trust – Discovery Educational Trust (DET).

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

- hard copy;
- email;
- secure extranet site(s) – AQA Centre Services; OCR Interchange; Pearson Edexcel Online; WJEC Secure Website;
- Management Information System (MIS) provided by ESS 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 examination entries, access arrangements, the conduct of examinations and Non-Examination Assessments (NEA), special consideration requests and examination results/post-results/certificate information.

3. Informing Candidates of the Information Held

CHS and SMS ensure that candidates are fully aware of the information and data held. All candidates are:

- informed via electronic communication and via the school websites;
- given access to this Policy if requested in writing.

Candidates are made aware of the above at the beginning of the academic year in which external examinations are to be taken, 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 is operating).

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 approval applications can be processed online.

4. Hardware and Software

IT hardware, software and access to online systems are protected in line with DPA 2018 and UK GDPR requirements. Protective measures include antivirus, regular maintenance and technical policies to control access to the internet.

Credentials for software/online systems are regularly maintained by the Network Manager and Centre Administrator, where relevant.

Both CHS and SMS have the ability to enable and disable spell-check and internet access on both desktop computers and on laptops, as necessary.

Also, where specialist software is required, i.e. Python, this is installed.

5. Dealing with Data Breaches

Although data is handled in line with DPA 2018 and 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, which holds it;
- cyber-attacks involving ransomware infections.

If a data protection breach is identified, the following steps are taken:

Containment and Recovery

The Data Protection Officer and Senior Information Risk Owner (SIRO) lead on investigating the breach.

The following is 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.

Assessment of Ongoing Risk

The following points are 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, is 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 that 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 provided?

Notification of Breach

Notification takes 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.

Evaluation and Response

Once a data breach has been resolved, a full investigation of the incident takes place. This includes:

- 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.

6. Candidate Information, Audit and Protection Measures

For the purposes of this Policy, all candidates' examinations-related information – even that not considered personal or sensitive under DPA 2018 and UK GDPR – is handled in line with DPA 2018 and UK GDPR guidelines.

An information audit is conducted annually, where all information that is no longer needed is securely shredded.

The table below details the type of candidate examinations-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 annually (this may include updating antivirus software, firewalls, internet browsers etc.).

7. 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 Examinations Archiving Policy, which is available on request.

8. Access to Information

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

The UK GDPR gives individuals the right to see information held about them. This means that individuals can request information about them and their examination performance, including:

- their mark;
- comments written by the examiner;
- minutes of any examination appeals panel.

This does not, however, give individuals the right to copies of their answers to examination questions.

Requesting Exam Information

Requests for examination information can be made to the Examinations Office via email. If a former candidate is unknown to staff, photo identification may be required.

The UK GDPR does not specify an age when a child can request their examination results, or request that they are not published. When a child makes a request, those responsible for responding should consider whether:

- the child wants their parent/carer (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 that 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 is made by the Head of Centre as to whether the student is mature enough to understand the request that they are making, with requests considered on a case-by-case basis.

Responding to Requests

If a request is made for examination information before examination results have been published, a request is 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 examination results have been published, the individual receives 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 is not 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, is 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 LA. The Centre's Data Protection Officer confirms the status of these agreements and approves/rejects any requests.

Sharing Information with Parents/Carers

The Centre considers any other legislation and guidance regarding sharing information with parents/carers (including non-resident parents and a Local Authority (the "corporate parent")). Refer example guidance from the 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-Aug-23 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 Examination Results

When considering the publication of examination results, CHS and SMS refer to the Information Commissioner’s Office (ICO) <https://ico.org.uk/your-data-matters/schools/exam-results/> Can schools give my exam results to the media for publication?

OR

CHS and SMS publish examination results to the media or within the Centre, for example, on an Honours Board) in line with the following principles:

- Refer to guidelines as published by JCQ;
- Act fairly when publishing results, and, where people have concerns about their or their child’s information being published, take those concerns seriously;
- Ensure that all candidates and their parents/carers are aware, as early as possible, whether examinations results are to be made public and how this will be done;
- Explain how the information is to be published. For example, if results will be listed alphabetically, or in grade order.

As CHS and SMS have a legitimate reason for publishing examination results, consent is not required from students or their parents/carers for publication. However, if a student or their parents/carers have a specific concern about publication of their results, they have the right to object. This objection must be made, in writing, to the Head of Centre, who considers the objection before deciding to publish and reply with a good reason to reject the objection to publish the examination results.

9. Table Recording Candidate Examinations-Related Information Held

For details of how to request access to information held, refer to Section 7 above.

For further details of how long information is held, refer to Section 6 above.

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 date of birth; 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; Secure user name and password; In secure office (Special Educational Needs and Disabilities Coordinator (SENDCo))	Until student reaches 25 years of age
Attendance registers (copies)		Candidate name	Files in Examinations Office	Locked door	Until Review of Results (ROR) deadline
Certificates		Candidate name Candidate date of birth	Envelopes in Examinations Office	Locked	1 year
Certificate issue information		Candidate name	Secure file on the server	Password	1 year
Conflicts of interest records		Candidate name	Secure file on the server	Password	1 year
Entry information		Candidate name Candidate date of birth	SIMS	Password	1 year
Invigilator and facilitator training records		Invigilator name	Secure file on the server	Password	1 year
Overnight supervision information		Candidate name	Secure file on the server	Password	1 year

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: confirmation of candidate consent information		Candidate name	Secure file on the server	Locked Examinations Office	1 year
Post-results services: requests/outcome information		Candidate name	Secure file on the server	Password	1 year
Post-results services: scripts provided by ATS service		Candidate name	Secure file on the server	Password	1 year
Results information		Candidate name Result	SIMS	Password	7 years