

# The Heathland School

*A Mathematics and Science College*



<b>General Data Protection Regulation policy (exams)</b>	<b>2022 - 2023</b>
Person(s) Responsible:	Headteacher, Deputy Head Curriculum, DPO
Status:	Statutory
Date Approved:	<b>January 2023</b>
Review Period:	As and when required

## Key staff involved in the General Data Protection Regulation policy

Role	Name(s)
Head of Centre	<b>Mr J M Rose</b>
Exams Officer	<b>Miss K Kundi</b>
Exams Officer Line Manager (Senior Leader)	<b>Mrs M Sandhu</b>
Data Protection Officer	<b>Mr M Rose</b>
IT Manager	<b>Mr W Sallah</b>
Data Manager	<b>Mrs A Srivastava</b>

## Purpose of the policy

This policy details how The Heathland 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 6.1)** 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.

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
- ▶ Department for Education
- ▶ Local Authority

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; EDUQAS; ASDAN; MENSA)
- ▶ Management Information System (MIS) provided Capita SIMS sending/receiving information via electronic data interchange (EDI) using A2C (<https://www.icq.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 Heathland School ensures that candidates are fully aware of the information and data held.

All candidates are:

- ▶ informed
- ▶ given access to this policy via centre website, written request

Candidates are made aware of the above at the start of their 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 Heathland School 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).

Candidates eligible for access arrangements 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.

## 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	<p>Checked repentantly by Network Manager</p> <p>Old hardware has been discontinued since it was over 12 years old and would not meet the security measures in place like Anti-virus and critical updates</p> <p>New hardware has been purchased which will be here from Oct/Nov this year</p> <p>Extra measures have been put in place to check on hardware devices every 4-6</p>	Oct 2023 for the 6 x new Laptop exams

	week to ensure that they are kept up to date with Anti-virus and critical updates	
--	---	--

Software/online system	Protection measure(s)
MIS; Internet browser(s); Awarding body secure extranet site(s); A2C	Protected usernames and passwords; rules for password setting (use of a mix of upper/lower cases letters and numbers); rules for regularity of password changing; centre administrator has to approve the creation of new user accounts and determine access rights; Extra measures have been put in place to check on hardware devices every 4-6 week to ensure that they are kept up to date with Anti-virus and critical updates

## 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

Mr Rose, 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 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 regularly (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 centre's Exams Archiving Policy which is available/accessible from the exams office(r).

## 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 Mrs Sandhu, Deputy Head (Curriculum) and or Miss Kundi, Examinations Officer in writing/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.

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 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 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.

We will not normally share personal data with anyone else, but may do so where:

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk
- We need to liaise with other agencies – we will seek consent as necessary before doing this
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies. When doing this, we will:
  - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
  - Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share
  - Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided.

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils or staff. Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

### **Sharing information with parents**

We do not share candidate examination results with Parents, or those with parental responsibility unless we have a written consent from the student.

There are certain circumstances in which this right can be denied, such as if releasing the information might cause serious harm to the physical or mental health of the pupil or another individual, or if it would mean releasing exam marks before they are officially announced.

### **Publishing exam results**

The Heathland School will publish exam results to the media or within the centre (e.g. on an honours board) in line with the following principles:

- Refer to guidelines as published by the Joint Council for Qualifications

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

As The Heathland School will 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 Mrs Sandhu, Deputy Head (Curriculum), who will consider the objection before making a decision to publish and reply with a good reason to reject the objection to publish the exam results.



## 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 Personal Data Consent (candidate signature) Diagnostic testing outcome(s) Specialist report(s) (may also include candidate address) Evidence of normal way of working	Access arrangements online MIS	In secure area solely assigned to exams/SENCo	
Alternative site arrangements	Any hard copy information generated on an alternative site arrangement. Notification submitted online via CAP.	Candidate name Candidate DOB Candidate number	In secure storage	Secure Storage - accessible by exams only	
Attendance registers copies		Candidate name Candidate number	In secure storage MIS	Secure Storage - accessible by exams only	
Candidates' work	Non-examination assessment work returned to the centre after awarding body at the end of the moderation period.				
Centre consortium arrangements for centre assessed work	Any hard copy information generated or relating to consortium arrangements for centre assessed work.				

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
	Applications submitted online via CAP.				
Certificates	A record of certificates that have been issued to candidates.	Candidate Name Candidate DOB Candidate number	In exams office	Exams Office - locked	
Certificate destruction information		Candidate Name Candidate DOB Candidate number	In exams office	Exams Office - locked	
Certificate issue information		Candidate Name Candidate DOB Candidate number Candidate signature	In exams office	Exams Office - locked	
Conflict of interest records	Records demonstrating the management of Conflicts of Interest	Candidate Name Candidate DOB Candidate number Staff Signature	In exams office Declaration email to awarding body	In secure area solely assigned to exams	
Entry information	Any hard copy information relating to candidates' entries.	Candidate Name Candidate DOB Candidate number	MIS		
Exam room incident logs	Logs recording any incidents or irregularities in exam rooms for each exam session.	Candidate Name Candidate DOB Candidate number	In Secure storage	Secure Storage - accessible by exams only	
Invigilator and facilitator training records		Invigilator name/DOB/signature	In exams office	Exams office - locked	

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	JCQ form <i>Timetable variation and confidentiality declaration for overnight supervision</i> for any candidate eligible for these arrangements.				
Post-results services: confirmation of candidate consent information	Hard copy or email record of required candidate consent	Candidate Name Candidate DOB Candidate number Candidate Signature	In the exams office MIS	In secure area solely assigned to exams	
Post-results services: requests/outcome information	Any hard copy information relating to a post-results service request (RoRs, appeals, ATS) submitted to an awarding body for a candidate and outcome information from the awarding body.	Candidate Name Candidate DOB Candidate number	In the exams office MIS	In secure area solely assigned to exams	
Post-results services: scripts provided by ATS service	Copies of exam scripts (or an electronic image of the script) returned to the centre by the awarding body/copies downloaded by the centre where the awarding body provides online access to scripts	Candidate Name Candidate DOB Candidate number	In the exams office MIS	In secure area solely assigned to exams	
Post-results services: tracking logs	Logs tracking to resolution all post-results service requests submitted to awarding bodies				
Private candidate information	<b>N/A</b>				
Resolving clashes information	Any hard copy information relating to the resolution of a	Candidate Name	In the exams office	In secure area solely assigned to exams	

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
	candidate's clash of timetabled exam papers	Candidate number	MIS		
Results information	Broadsheets of results summarising candidate final grades by subject by exam series.	Candidate name Candidate DOB Gender Candidate number	MIS	In secure area solely assigned to exams	
Seating plans	Plans showing the seating arrangements of all candidates for every exam taken.	Candidate name Candidate number	In secure storage MIS	Secure Storage - accessible by exams only	
Special consideration information	Any hard copy information relating to a special consideration request and supporting evidence submitted to an awarding body for a candidate	Candidate name Candidate DOB Gender Candidate number	Applications submitted online via CAP. MIS	In secure area solely assigned to exams	
Suspected malpractice reports/outcomes	Any hard copy information relating to a suspected or actual malpractice investigation/report submitted to an awarding body and outcome information from the awarding body.	Candidate name Candidate DOB Gender Candidate number	In secure area solely assigned to exams	In secure area solely assigned to exams	
Transferred candidate arrangements	Any hard copy information relating to a transferred candidate arrangement. Applications submitted online via CAP.	Candidate name Candidate DOB Gender Candidate number	Applications submitted online via CAP. MIS	In secure area solely assigned to exams	

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
Very late arrival reports/outcomes	Any hard copy information relating to a candidate arriving very late to an exam. Reports submitted online via CAP.	Candidate name Candidate DOB Gender Candidate number	Applications submitted online via CAP.  MIS	In secure area solely assigned to exams	