GREATFIELDS SCHOOL

General Data Protection Regulation policy (exams)

Head of Centre	**Mr Richard Paul**
SLT member with responsibility:	**Mr Matthew Gillham**
Approved by SLT:	**Date: September 2021**
Next Review Date:	**September 2022**

**This policy is reviewed annually to ensure compliance with current regulations.*

Purpose of the policy

This policy details how Greatfields, in relation to exams management and administration, ensures compliance with the regulations as set out by the Data Protection Act 2018 (DPA 2018) and General Data Protection Regulation (GDPR).

> 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's General Regulations for Approved Centres (GR, 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
- not transferred outside the European Economic Area without adequate protection

To ensure that the centre meets the requirements of the DPA 2018 and 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 – Candidate information, audit and protection measures*.

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

- Awarding bodies
- Joint Council for Qualifications
- Department for Education; Local Authority
- External Assessors

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

- hard copy
- email
- secure extranet site(s) –eAQA; OCR Interchange; Pearson Edexcel Online; WJEC Secure services, etc.
- 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; etc.]

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

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

All candidates are:

- given access to this policy centre website or written request.

Candidates are made aware of the above at the start of their course of study leading to an externally accredited qualification.

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 GDPR.

Candidates eligible for access arrangements 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 software and access to online systems is protected in line with DPA & GDPR requirements.

Software/online system	Protection measure(s)
MIS	regularity of password changing, centre administrator has to approve the creation of new user accounts and determine access rights. protected usernames and passwords, use of a mix of upper/lower cases letters and numbers
Awarding body secure extranet site	protected usernames and passwords, use of a mix of upper/lower cases letters and numbers, regularity of password changing; centre administrator has to approve the creation of new user accounts and determine access rights; regular checks to Firewall/Antivirus software.
A2C	protected usernames and passwords, use of a mix of upper/lower cases letters and numbers regularity of password changing; centre administrator has to approve the creation of new user accounts and determine access rights. Files are zipped and encrypted during transportation.
Files	Encrypted, logged, files are sent via zipped/compressed.
internet	Regular checks to Firewall/Antivirus software.

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

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

1. **Containment and recovery**

A member of the SLT 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.

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 2 months (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 [please refer to our Exams archiving policy] which is available/accessible from the exams officer and in our Exams Policy.

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 results, 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 Exams Officer in an 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.

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 results have been announced, 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), as 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
- School reports on pupil performance

www.gov.uk/guidance/school-reports-on-pupil-performance-guide-for-headteachers

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**)

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
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 In secure office (SENDCo)	Retained until the post-results period has been completed for that exam series
Alternative site arrangements	For external exams or space issues.	• Candidate name • Candidate number • Gender	Lockable filing cabinet	Only accessible by EO staff	Retained until the post-results period has been completed for that exam series
Attendance registers copies	Registers record attendance at each written exam, are kept with seating plan and exam room incident log	• Candidate name • Candidate number • Presence at exam Lockable filing cabinet Only accessible by EO staff	Lockable filing cabinet	Only accessible by EO staff	To be retained until the deadline for EARs or the resolution of any outstanding enquiries/appeals
Candidates' work	Controlled assessments, coursework and nonexamination assessments	Candidate name Candidate number Candidate marks and grades	Lockable filing cabinet	Only accessible by EO staff	Retained until the post-results period has been completed for that exam series

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
Certificates	Record of achievement	Candidate name Candidate number UCI number Candidate ODB Candidate marks and grades	Lockable filing cabinet	Only accessible by EO staff	Retained securely for a minimum of 12 months from date of issue
Certificate destruction information	A record of unclaimed certificates that have been destroyed.	Candidate name Candidate number UCI number Candidate ODB Candidate marks and grades	In Exams R:Drive > Archive	Access rights to EO	To be retained for 4 years from the date of certificate destruction
Certificate issue information	A record of certificates that have been issued to candidates.	Candidate name Candidate number Candidate qualifications	Certificate collection file. Copies of post receipts or student's sign-out in person, scanned and saved in file.	Access rights to EO	To be retained for 4 years from the date of certificate destruction
Conflicts of Interest records	A form and Log	Candidate/staff name Candidate/staff number Candidate/staff qualifications	Lockable filing cabinet	HoC and EO	Retained securely for a minimum of 12 months from date of issue or outstanding enquiries/appeals for the relevant exam's series
Entry information	A record of which qualifications candidates have been entered for.	Candidate name, number, exam number, programme of study, qualification information	SIMS **Electronic Exams folder**	Access rights to EO, Techers, SLT, HoC	Retained until the post-results period has been completed for that exam series

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
Exam room incident logs	Logs detailing the chronological activity happening in exam rooms from start to finish	Candidate name Candidate number Reason for leaving the room	With the corresponding attendance register and seating plan in lockable filing cabinet	Only accessible by EO, HoC/DHoC staff	To be retained until the deadline for EARs or the resolution of any outstanding enquiries/appeals for the relevant exams series.
Invigilator and facilitator training records				EO and DHoC only	
Overnight supervision information	Copy of JCQ form Timetable variation and confidentiality declaration for overnight supervision for any candidate eligible for these arrangements	Candidate name , number and address	Electronically in exams folder	EO AND DHoC only	To be retained indefinitely for JCQ inspection purposes.
Post-results services: confirmation of candidate consent information	Hard copy or email record of candidate consent for an EAR or ATS request to be submitted to an awarding body	Candidate name Candidate number Candidate results information	Post-results services file for relevant academic year	Only accessible by EO staff. Only shared with HoD/HoC / DHoC	EAR consent to be retained for at least six months following the outcome of the enquiry or any subsequent appeal. ATS consent to be retained for at least six months from the date consent given.

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
Post-results services: requests/outcome information	Any hard or digital copies of information relating to a post-results service request (EARs, appeals, ATS) submitted to an awarding body for a candidate and outcome information from the awarding body	Candidate name Candidate number Candidate results information	Post-results services file for relevant academic year	Only accessible by EO staff. Only shared with HoD/HoC/ DHoC	Retained for at least six months following the outcome of the enquiry or any subsequent appeal.
Post-results services: scripts provided by ATS service	Copy, digital or original exam scripts returned to the centre by the awarding body.	Candidate name Candidate number Candidate results information	Where scripts are retained by the centre, they are securely stored (including any electronic versions) and not edited in any way or disposed of until after the awarding body deadline.	Only accessible by EO staff.	n/a returned to the requester after the post results period is complete
Post-results services: tracking logs	A log tracking to resolution all post-results service requests submitted to awarding bodies	Candidate name Candidate number Candidate results information	Post-results services file for relevant academic year	Only accessible by EO staff.	Retained for at least six months following the outcome of the enquiry or any subsequent appeal.
Resolving timetable clashes information	Any information relating to the resolution of a candidate's clash of exam	Candidate name, candidate number	Electronically on exams folder	EO Only	To be retained until the deadline for EARs or the resolution of any

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
	papers or a timetable variation				outstanding enquiries/appeals for the relevant exams series.
Results information	Broadsheets of results summarising candidate final grades by subject by exam series.	Candidate name, candidate number, DOB, gender, result information	SIMS, electronic folder for Exams in Results(academic year)	EO, DHoC only	Records for current year plus previous 5 years to be retained as a minimum.
Seating plans	Plans showing the seating arrangements of all candidates for every exam taken	Candidate name Candidate number Candidate toilet breaks	With the corresponding attendance register and incident log in lockable filing cabinet	EO only	To be kept until the deadline for EARs and the resolution of any outstanding enquiries/appeals for the relevant exams series.
Special consideration information	Any hard or digital copies of information relating to a special consideration request and supporting evidence submitted to an awarding body for a candidate.	Candidate name Candidate number Candidate date of birth Candidate medical information	Lockable filing cabinet	EO, SENDCo, EAL, DHoC only	To be kept until the deadline for EARs and the resolution of any outstanding enquiries/appeals for the relevant exams series.

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
Suspected malpractice reports/outcomes	Any hard or digital copies of information relating to a suspected malpractice investigation/report submitted to an awarding body and outcome information from the awarding body.	Candidate name Candidate number	On Exams R:Drive, filed by Academic Year > Malpractice	EO, HoC, DHoC	To be kept until the deadline for EARs and the resolution of any outstanding enquiries/appeals for the relevant exams series.
Transferred candidate arrangements	Transferred candidate arrangements	Candidate name Candidate number Candidate UCI	In Exams R:Drive > Transfer of credit	EO, HoC, DHoC	To be retained until the transfer arrangements are confirmed by the awarding body.
Very late arrival reports/outcomes	Very late arrival reports/outcomes	Candidate name Candidate number	In Exams R:Drive > Academic Year > Very late arrivals	EO, HoC, DHoC	To be kept until the deadline for EARs and the resolution of any outstanding enquiries/appeals for the relevant exams series.

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