Greenhead College Corporation

Examinations General Data Protection Regulation Policy 21/22

Key staff involved in the Exams GDPR policy

Role	Name(s)
Head of centre	**S Lett**
Exams Manager	**M Darlington**
Deputy Principal (line manager)	**M Bunter**
Data Protection Officer	**J Blake**
Director of Information Services	**P Diamond**
Network Manager	**R Lyons**

Purpose of the policy

This policy details how Greenhead College, 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 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 General Regulations for Approved Centres (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

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 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* below.

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

- Awarding bodies
- Joint Council for Qualifications
- Department for Education, ALPS

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

- hard copy
- email
- secure extranet sites: AQA Centre Services; OCR Interchange; Pearson Edexcel Online; WJEC Secure Website; Cambridge Assessment Extranet
- Unit-E 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, special consideration requests and exam results/post-results/certificate information.

Section 2 – Informing candidates of the information held

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

All candidates are:

- informed via the enrolment process
- given access to this policy via centre website, centre intranet Moodle

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

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 2019 and UK GDPR. This is included in the examinations guidance and procedures booklet issued to all candidates.

Candidates eligible for access arrangements which require awarding body approval 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 in the exams department

The table below confirms how IT hardware, software and access to online systems is protected in line with DPA & GDPR requirements. The exams office is locked when unoccupied. All computers are password-protected.

Hardware	Date of purchase and protection measures	Warranty expiry
• Exams Office: three Desktop computers • Exams Manager: laptop	Network Manager is the records owner	Network Manager is the records owner

Software/online system	Protection measure(s)
• Exam results (1) • Cedar (2) • MOODLE (Intranet) (3) • Unit-e (4)	(1) If stored on the F Drive, are accessible to administrative staff online; if stored on the R Drive, are accessible to exams staff only (2) This password-protected software is accessible (with restrictions) to all staff and students. Students can only see their own data (3) This password-protected software is accessible (with restrictions) to all staff and students (4) This password-protected software is accessible (with restrictions) to some support staff and all exams staff
• Awarding body secure extranet sites (1) • A2C (2)	(1) This password-protected software is accessible to Exams staff, SLT, members of teaching staff and the ALS Manager, with differing access rights depending on role. Exams Manager is the centre administrator; he reviews the users annually, determines access rights, and deletes staff leavers. (2) The Exams Manager has access to A2C; this is restricted to the Exam Manager's desktop computer in a locked exams office.

• Computer files and data	Exams staff have password protected access to their desktops. Files containing personal data are held in restricted access folders (F drive and R drive)

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

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

An information audit is conducted annually by the Exams Manager and Exams Officers.

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 at the discretion of the Network Manager, including 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 'gc Examinations Archiving Policy 2021 – 2022' which is available/accessible from the Exams Manager. The ALS Manager is the records owner for all access arrangements documentation.

Section 7 – Access to information

Current and former candidates can request access to the information/data held on them by making an **access request** to the College Reception staff in writing, by e-mail or in person. ID is requested prior to any information being given. All requests will be dealt with within 40 calendar days.

Third party access

Permission must 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 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 Data Protection Officer will confirm the status of these agreements and approve/reject any requests.

Author:	*Exams Manager (MDA)*
Date drafted:	*October 2021*
Date of next review:	*October 2024*