Examination Policy

The Holgate Academy

Edition – September 2023

We empower | We respect | We care

Diverse Academies

Contents

Key staff involved in the General Data Protection Regulation policy

Role	Name(s)
Principal	Mr H Diamond
Exams officer	Mrs K Evans
Exams officer line manager	Mr R Ellis
Data Protection Officer	Mrs A Elway
IT manager	Mr P Richardson

Purpose of the policy

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

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 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
- DfE
- Alternative Provision organisations
- Local press /media - Press releases

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

- hard copy via secure mail methods ie Royal Mail signed for, tracked
- encrypted email
- secure extranet site(s) – eAQA; OCR Interchange; Pearson Edexcel Online; WJEC Secure services; NCFE
- Management Information System (MIS) provided by Capita SIMS
- sending/receiving information via secure 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

The Holgate Academy ensures that candidates are fully aware of the information and data held.

All candidates are:

- informed via letter
- given access to this policy via our website

Candidates are made aware of the above on entry to the academy and during their time in school

Section 3 – 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**

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 4 – 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.

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 periodically (this may include updating antivirus software, firewalls, internet browsers etc).

Section 5 – Data retention periods

Details of retention periods, the actions taken at the end of the retention period and method of disposal information is available from the Examinations Officer.

Section 6 – 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 academy, full details are available via a link to DALP on our website.

Third party access

Permission should be obtained before requesting personal information on another individual from a third-party organisation.

Candidates' personal data will only be shared with a third party in accordance with our GDPR policy.

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 7 – Review

Published: June 2023	**Next review:** June 2024	**Statutory/non:** Non-statutory	**Lead:** Rich Ellis (Assistant Head)
Associated documents:			
Links to:			