GDPR (Exams) Policy

Policy Control Page

Responsible Person	Claire Quick – Director Finance & Resources (The Deaf Academy Data Protection Officer)
Approved By	Claire Quick – Director Finance & Resources (The Deaf Academy Data Protection Officer)
Date of Last Approval	October 2022
Next Review Date	October 2023
Policy Applicable to	Education
Status	Approved

Date	Version	Person	Change / Action
March 2019	V1	Salena Hutton	Policy Created
October 2020	V2	Salena Hutton	Review and update policy to meet JCQ
October 2021	V3	Salena Hutton	Review and update policy to meet JCQ
October 2022	V4	Salena Hutton	Review and update policy to meet JCQ

Purpose of the policy

This policy details how Exeter Royal Academy for Deaf Education (The Academy) 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 *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.

Students are given the right to find out what information the Academy 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 Academy 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 officer 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
- Relevant Local Authority

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

- hard copy
- email
- secure extranet site(s) –e.g. eAQA; OCR Interchange; Pearson Edexcel Online; WJEC Secure services; Signature Academy Portal
- Management Information System (MIS) provided by Capita, Scomis via 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 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 Academy ensures that candidates are fully aware of the information and data held.

All candidates are:

- informed via information provided in the Academy "Permissions Booklet"
- given access to this policy via a written request to the Data Co-Ordinator
- made aware of the above via the "Permissions Booklet" sent annually to students, their parents, guardians and/or carers

The Academy 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, as part of qualification information to students and their parents, guardians and/or carers

Candidates eligible for access arrangements which require awarding body approval using Access Arrangements Online are also required to provide their consent by

signing the UK GDPR compliant JCQ candidate personal data consent form before access arrangements approval applications can be processed online. This is also included in the "Permissions Booklet".

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	Sept-2016. Limited user account. Anti-virus protection updated daily	N/A

Software/online system	Protection measure(s)
S Drive	Protected usernames and passwords. Regular checks to firewall and anti virus software.
Academy Sharepoint and MS Teams	Protected usernames and passwords. Regular checks to firewall and anti virus software.
Internet Browser	Protected usernames and passwords. Regular checks to firewall and anti virus software.
Awarding Body's Secure Extranet Sites	Protected usernames and passwords. Academy Administrator has to approve the creation of new user accounts and determine access rights;
SIMS	Protected usernames and passwords with enforced password changes regularly. Remote desktop system protection by Scomis.

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 to 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.

The table below details the type of candidate exams-related information held, and how it is managed, stored and protected

Protection measures may include:

- Candidate information is stored on a server in an access controlled secure room. Access to the server is controlled by Active Directory user accounts and is restricted to essential staff.
- Passwords for Active Directory user accounts are required. Updates to servers are performed weekly, sometimes more often if there are any urgent patches/updates.
- Client computers download Windows updates every week and are performed a convenient time to users. Antivirus is installed on every client computer and is updated daily.
- An organisational firewall is installed protecting all internal clients, and the local Windows firewall is also enabled.

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 Academy's Exams archiving policy, which is available from the Exams Officer

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 the Data Protection Officer in writing or by email. ID will need to be confirmed if a former candidate is unknown to current staff.

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 the Academy Principal 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 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.

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, 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 Local Authority). The Academy's Data Protection Officer will confirm the status of these agreements and approve/reject any requests.

Sharing information with parents

The Academy 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 7 – 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	What personal/sensitive data is/may be contained in the information	Where information is stored	How information is protected
Access arrangements information	Candidate name Candidate DOB Gender Data protection notice (candidate signature)	Access Arrangements Online S drive	Secure user name and password Secure user name and password. Secure folders

Information type	What personal/sensitive data is/may be contained in the information	Where information is stored	How information is protected
	Specialist report(s) (may also include candidate address) Evidence of normal way of working	Lockable metal filing cabinet	In administration office, with limited access
Attendance registers copies	Candidate name Candidate number	Locked cabinet within admin office	Locked cabinet
Candidates' scripts	Candidate name Candidate number	Locked safe within admin office until dispatched	Locked safe
Candidates' work	Candidate name Candidate number	Stored by teacher in secure room within classroom Stored in secure room solely for exam purposes S Drive	Secure room Secure store Secure user name and password. Secure folders
Certificates	Candidate name	Stored in locked cupboard within Admin Office S Drive	Locked cupboard Secure user name and password. Secure folders
Certificate issue information	Candidate name (Note: Given to students at leavers' assembly or posted home via recorded delivery)	S Drive	Secure user name and password. Secure folders
Conflicts of Interest records	Staff name Staff DOB Staff Address	S Drive	Secure user name and password. Secure folders

Information type	What personal/sensitive data is/may be contained in the information	Where information is stored	How information is protected
Entry information	Candidate name Candidate DOB Candidate number	S Drive	Secure user name and password. Secure folders
Exam room incident logs	Candidate name Candidate number	Locked cabinet within admin office	Locked cabinet
Invigilator and facilitator training records	Staff name Staff DOB	Locked cabinet within admin office	Locked cabinet
Overnight supervision information	Candidate name Candidate DOB Candidate number Candidate address	Locked cabinet within admin office S Drive	Locked cabinet Secure user name and password. Secure folders
Post-results services: confirmation of candidate consent information	Candidate name Candidate DOB Candidate number	Locked cabinet within admin office S Drive	Locked cabinet Secure user name and password. Secure folders
Post-results services: requests/outcome information	Candidate name Candidate DOB Candidate number	Locked cabinet within admin office S Drive	Locked cabinet Secure user name and password. Secure folders
Post-results services: scripts provided by ATS service	Candidate name Candidate DOB Candidate number	Locked cabinet within admin office S Drive	Locked cabinet Secure user name and password. Secure folders
Resolving timetable clashes information	Candidate name Candidate DOB Candidate number	Locked cabinet within admin office S Drive	Locked cabinet Secure user name and password. Secure folders

Information type	What personal/sensitive data is/may be contained in the information	Where information is stored	How information is protected
Results information	Candidate name Candidate DOB Candidate number	S Drive SIMS	Secure user name and password. Secure folders Secure user name and password.
Seating plans	Candidate name Candidate number	Locked cabinet within admin office	Locked cabinet
Special consideration information	Candidate name Candidate DOB Candidate number	Locked cabinet within admin office	Locked cabinet
Suspected malpractice reports/outcomes	Candidate name Candidate DOB Candidate number	Locked cabinet within admin office	Locked cabinet
Very late arrival reports/outcomes	Candidate name Candidate number	Locked cabinet within admin office	Locked cabinet