



Title:	General Data Protection Regulation Policy (Exams)
Internal Reference:	L4L-GY-042
Approved by:	Sara Morris
Issue Date:	September 2020
Version No:	V1
Review Date:	September 2024

General Data Protection Regulation Policy (Exams)

Key staff involved in the General Data Protection Regulation Policy

Role	Name(s)
Head of Centre	Claire Smith
Curriculum Lead	
Exams Officer	Tala Alhuraibat
Data Protection Officer	Sara Morris

Purpose of the policy

This policy details how Learning4life-GY, 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).

Learners 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 (including OCR and NOCN)
- ▶ Joint Council for Qualifications
- ▶ North East Lincolnshire Council
- ▶ Skills Funding Agency
- ▶ Ofsted
- ▶ Department for Education

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

- ▶ hard copy
- ▶ email
- ▶ secure extranet site(s) – e.g. OCR Interchange; NOCN Secure Services
- ▶ Management Information System (MIS) provided by sending/receiving information via electronic data interchange (EDI) using A2C (<https://www.jcq.org.uk/about-a2c>) to/from awarding body processing systems; MAYTAS and Goldmine

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

Learning4life-GY ensures that candidates are fully aware of the information and data held.

All candidates are:

- ▶ via the Centre's newsletter
 - given access to this policy via the Centre's website or through written request

Candidates are made aware of the above, during the enrolment process and again, at the start of their course of study leading to examinations.

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

The table below confirms how IT hardware, software and access to online systems are protected in line with DPA & GDPR requirements.

Hardware	Date of purchase and protection measures	Warranty expiry
Desktop computer	Purchase date – ongoing Protection measures include annual hardware checks via IT Services. These checks include hard drive scans; antivirus protection up to dates etc.	N/A – reviewed via IT Services
Agile kit (including laptops, tablets, and mobile phones)	Purchase date – ongoing Protection measures include annual hardware checks via IT Services. These checks include hard drive scans; antivirus protection up to dates etc.	N/A – reviewed via IT Services

Software/online system	Protection measure(s)
MIS	Protected usernames and passwords; rules for password setting (i.e. 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; regular checks to Firewall/Antivirus software; etc.
Intranet	Protected usernames and passwords; rules for password setting (i.e. 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; regular checks to Firewall/Antivirus software; etc.
Internet browser(s)	Protected usernames and passwords; rules for password setting (i.e. 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; regular checks to Firewall/Antivirus software; etc.
Awarding Body secure extranet site(s); A2C; OCR Interchange; NOCN Secure Services	Protected usernames and passwords; rules for password setting (i.e. 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; regular checks to Firewall/Antivirus software; etc.

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

Sara Morris – Director, 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.

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 3 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 Exams Archiving Policy.

Section 7 – Access to information

Current and former candidates can request access to the information/data held on them by making a **subject access request** to Sara Morris in writing. All requests will be dealt with within 40 calendar days.

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 are already in place for information to be shared with the relevant authorities. Sara Morris will confirm the status of these agreements and approve/reject any requests.

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 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 area solely assigned to exams	
Attendance registers copies		Candidate name Candidate number	Filing Cabinet in secure room		To be stored safely and securely until after the deadline for EARs or the resolution of any outstanding enquiry/appeal or malpractice investigations for the exam series
Candidates' scripts	Exam scripts	Candidate name Candidate number Exam answers	Filing Cabinet in secure room	In secure area solely assigned to exams. When being transferred to the exam board from centre, is sent via	Exam papers are retained until the end of the exam day or next working day, where they are then posted

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
				the courier service Parcelforce. If the courier service is not used then they are transported to the Post Office by an authorised staff member who will obtain a receipt of dispatch.	to the relevant exam board.
Candidates' work	Non-examination assessment work (inc. controlled assessment, coursework, portfolios) returned to the Centre following Awarding Body moderation	Candidate name Candidate number	To be immediately returned to subject staff as records owner. To be stored safely and securely along with work that did not form part of the moderation sample (including materials stored electronically) until after the deadline for EARs or the resolution of any outstanding enquiry/appeal or malpractice investigations for the exam series.	Each Tutor stores assessment work in secure cupboard	Returned to candidate or safe disposal
Certificates		Candidate name Candidate DOB Candidate examination results	In Exams office	Limited number of key holders to office	7 years from date of issue
Certificate destruction information	A record of unclaimed certificates that have been destroyed	Candidate name Candidate DOB Candidate examination results	In Exams office	Limited number of key holders to office	7 years from date of issue

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
Certificate issue information	A record of certificates that have been issued to candidates	Candidate name Candidate DOB Candidate examination results	In Exams office	Limited number of key holders to office	7 years from date of issue
Entry information	Any hard copy information relating to candidates' entries	Candidate name Candidate DOB Candidate examination results	In Exams office	Limited number of key holders to office	To be stored safely and securely until after the deadline for EARs or the resolution or any outstanding enquiry/appeal or malpractice investigations for the exam series
Exam room incident logs	Logs recording any incidents or irregularities in exam rooms	Candidate name Candidate DOB	In Exams office	Limited number of key holders to office	To be stored safely and securely until after the deadline for EARs or the resolution or any outstanding enquiry/appeal or malpractice investigations for the exam series
Overnight supervision information	N/a	N/a	N/a	N/a	N/a
Post-results services: confirmation of candidate consent information	Hard copy or email record of candidate consent for EAR or ATS request to be submitted to an Awarding Body	Candidate name Candidate exam number	In Exams office	Limited number of key holders to office	EAR consent to be retained for at least six months following the outcome of the

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
					enquiry or any subsequent appeal / malpractice investigations for the exam series. ATS consent to be retained for at least six months from the date consent given.
Post-results services: requests/outcome information	Any hard copy 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 exam number	In Exams office On Exams office computer	Limited number of key holders to office	To be stored safely and securely until after the deadline for EARs or the resolution or any outstanding enquiry/appeal or malpractice investigations for the exam series
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 exam number	To be immediately provided to the Head of Centre, or the candidate as records owner		
Post-results services: tracking logs	A log tracking to resolution all post-results service requests submitted to Awarding Bodies	Candidate name Candidate number	Exams office computer	Only accessible by Exams Officer log-in	Retained for 12 months after the deadline for EARs

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
Private candidate information	N/a	N/a	N/a	N/a	N/a
Resolving clashes information	Any hard copy information relating to the resolution of a candidate's clash of exam papers or a timetable variation	Candidate name Candidate exam number	On Exams office computer	Exams Officer only log in	To be stored safely and securely until after the deadline for EARs or the resolution or any outstanding enquiry/appeal or malpractice investigations for the exam series
Results information	Broadsheets of results summarising candidate final grades by subject and by exam series	Candidate name Candidate number	Exams office computer Filing cabinets	Exams Officer only log in Secure office	7 years
Seating plans	Plans showing the seating arrangements of all candidates for every exam taken	Candidate name Candidate number	Exams office computer Exams office	Exams Officer only log in Secure office	To be stored safely and securely until after the deadline for EARs or the resolution or any outstanding enquiry/appeal or malpractice investigations for the exam series
Special consideration information	Any hard copy information relating to a special consideration request and supporting evidence	Candidate name Candidate number Candidate DOB Candidate address	Filing cabinet Exams office		To be stored safely and securely until after the deadline for EARs or the

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
	submitted to an Awarding Body for a candidate	Candidate personal or medical information			resolution or any outstanding enquiry/appeal or malpractice investigations for the exam series
Suspected malpractice reports/outcomes	Any hard copy information relating to a suspected malpractice investigation/report submitted to an Awarding Body and outcome information from the Awarding Body	Candidate name Candidate number Candidate DOB Detail of the malpractice	Exams office		Retained until after the deadline for EARs or until any appeal, malpractice or other results enquiry has been completed whichever is later
Transfer of credit information	N/a	N/a	N/a	N/a	N/a
Transferred candidate information	Any hard copy information relating to an application for a transferred candidate arrangement submitted to an Awarding Body for a candidate	Candidate name Candidate number Candidate DoB			Retained until after the deadline for EARs or until any appeal, malpractice or other results enquiry has been completed whichever is later
Very late arrival reports/outcomes	Any hard copy information relating to a very late arrival report submitted to an Awarding Body for a candidate and outcome information from the Awarding Body	Candidate name Candidate number			Retained until after the deadline for EARs or until any appeal, malpractice or other results

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
					enquiry has been completed whichever is later