

# General Data Protection Regulation policy (exams)

2017/18

This policy is annually reviewed to ensure compliance with current regulations

<b>Approved/reviewed by</b>	
<b>Date of next review</b>	

## Key staff involved in the General Data Protection Regulation policy

Role	Name(s)
Head of centre	<b>Mark Allchorn</b>
Exams officer	<b>Becky Fenson</b>
Exams officer line manager (Senior Leader)	<b>Scarlett O’Sullivan</b>
Data Protection Officer	
IT manager	<b>Tariq Bizanjo</b>
Data manager	

### Purpose of the policy

This policy details how [insert centre name], 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(x) 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
- ▶ [insert (by listing) any other organisations as relevant to your centre e.g. Department for Education; Local Authority; Multi Academy Trust; Consortium; the Press; etc.]

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

- ▶ hard copy
- ▶ email
- ▶ secure extranet site(s) – [insert as appropriate to your centre e.g. eAQA; OCR Interchange; Pearson Edexcel Online; WJEC Secure services; City & Guilds Walled Garden; etc.]
- ▶ [insert any other methods as appropriate to your centre e.g. a Management Information System (MIS) provided by [insert MIS provider detail (e.g. 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

[Insert centre name] ensures that candidates are fully aware of the information and data held.

All candidates are:

- ▶ informed via [insert how e.g. centre newsletter, electronic communication, etc.]
- ▶ given access to this policy via [insert how e.g., centre website, written request, etc.]

Candidates are made aware of the above [insert when e.g. at the start of their course of study leading to external examinations].

## 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
IT-LAPTOP01 - 3F257956C	APR 17 - 2015 03/05/18 - Version 10.3	APR 16 - 2016
IT-LAPTOP12 - XF071337C	OCT. 29 - 2015 03/05/18 - Version 10.3	OCT 28 - 2016
IT-LAPTOP05 - XF071316C	OCT. 29 - 2015 03/05/18 - Version 10.3	OCT. 28 - 2016
IT-LAPTOP04 - XF071381C	OCT. 29 - 2015	OCT 28 - 2016

**GDPR policy (exams) template (2017/18)**

Hyperlinks provided in this document were correct as at February 2018

	03/05/18 - Version 10.3	
IT-LAPTOP14 - 3F257981C	APR 17 - 2015 03/05/18 - Version 10.3	APR 16 - 2016
IT-LAPTOP15 - CND75128S6	Feb-18 03/05/18 - Version 10.3	Unknown
IT-LAPTOP16 - CND75128M5	Feb-18 03/05/18 - Version 10.3	Unknown
IT-LAPTOP07 - 3F258025C	APR 22 - 2015 03/05/18 - Version 10.3	APR 21 - 2016
IT-LAPTOP17 - CND75128QZ	Feb-18 03/05/18 - Version 10.3	Unknown
IT-LAPTOP10 - XF071374C	OCT. 29 - 2015 03/05/18 - Version 10.3	OCT. 28 - 2016
IT-LAPTOP18 - CND75128J5	Feb-18 03/05/18 - Version 10.3	Unknown
IT-LAPTOP06 - XF071368C	OCT. 29 - 2015 03/05/18 - Version 10.3	OCT. 28 - 2016
ITLAPTOP13 - 3F257948C	APR 17 - 2015 03/05/18 - Version 10.3	APR 16 - 2016
DESKTOP MANLYNNP - 4Q9RV02	APRIL 4TH - 2014 03/05/18 - Version 10.3	APRIL 04 - 2017

Software/online system	Protection measure(s)
SIMS	Secure login, antivirus software & firewall
A2C	Secure login, antivirus software & firewall
4Matrix	Secure login, antivirus software & firewall
Edexcel	Secure login, antivirus software & firewall
AQA	Secure login, antivirus software & firewall
OCR	Secure login, antivirus software & firewall
WJEC	Secure login, antivirus software & firewall
NCFE	Secure login, antivirus software & firewall

## 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**

[Insert staff name and/or role e.g. 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 [detail the regularity].

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 [XX] 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 [insert e.g. Exams archiving policy] which is available/accessible from [insert who and/or where].

## 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 [insert staff name and/or role e.g. the Data Protection Officer] in [insert how e.g. writing/email and how ID will need to be confirmed if a former candidate is unknown to current staff]. 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 [insert your centre's process for sharing data with a third-party e.g. 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.

## 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 [insert] In secure area solely assigned to exams	
Attendance registers copies		Candidate name Candidate number	Lockable metal filing cabinet		To be stored safely and securely until after the deadline for EAR's or the resolution of any outstanding enquiry's/appeal or malpractice investigations for the exam series.
Candidates' work	Non-examination assessment work (inc. controlled assessments, coursework, portfolios)	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	Each department stores in secure cupboard.	Returned to candidates or safe disposal.

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
	returned to centre after moderation.		part of the moderation sample (including materials stored electronically) until after the deadline for EAR's or the resolution of any outstanding enquiry's/appeal or malpractice investigations for the exam series.		
Certificates		Candidate name Candidate DOB Candidate examination results	In the exams office	Limited to 4 key holders	Indefinitely
Certificate destruction information	. N/A	N/A	N/A	N/A	N/A
Certificate issue information	A record that certificates have been issued to candidates.	Candidate name Candidate DOB	In the exams office	Limited to 4 key holders	Indefinite
Entry information	Any hard copy information relating to candidates entries	Candidate name Candidate number	In the exams office	Limited to 4 key holders	To be stored safely and securely until after the deadline for EAR's or the resolution of any outstanding enquiry's/appeal or malpractice investigations for the exam series.

<b>Information type</b>	<b>Information description (where required)</b>	<b>What personal/sensitive data is/may be contained in the information</b>	<b>Where information is stored</b>	<b>How information is protected</b>	<b>Retention period</b>
Exam room incident logs		Candidate name Candidate number	In the exams office	Limited to 4 key holders	To be stored safely and securely until after the deadline for EAR's or the resolution of any outstanding enquiry's/appeal or malpractice investigations for the exam series.
Overnight supervision information		Candidate name Candidate number Candidate address details	In the exams office		To be stored safely and securely until after the deadline for EAR's or the resolution of any outstanding enquiry's/appeal or malpractice investigations for the exam series.
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 email address	In the exams office	Limited to 4 key holders	To be stored safely and securely until after the deadline for EAR's or the resolution of any outstanding enquiry's/appeal or malpractice

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
					investigations for the exam series.
Post-results services: requests/outcome information	Any hard copy information relating to post-results services (EARs, appeals or ATS) submitted to an awarding body for a candidate and outcome information from the awarding body.	Candidate name Candidate number	In the exams office On the exam office computer	Limited to 4 key holders Password protection on awarding body online sites.	To be stored safely and securely until after the deadline for EAR's or the resolution of any outstanding enquiry's/appeal or malpractice investigations for the exam series.
Post-results services: scripts provided by ATS service	<b>Copies of exam scripts (or an electronic image of the script) returned to the centre by the awarding body/copied downloaded by the centre where the awarding body provides online access to scripts.</b>	Candidate name Candidate number	To be immediately provided to the head of department or the candidate as records owner		
Post-results services: tracking logs	<b>A log tracking to resolution all post-results service requests submitted to awarding bodies.</b>	Candidate name Candidate number	On exam office computer/hard copy log in the exams office	Password protected on exams officer log in/limited to 4 key holders	To be stored safely and securely until after the deadline for EAR's and the resolution of any outstanding enquiry's/appeal or malpractice investigations for the 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 period
Private candidate information	<b>Any hard or digital copy information relating to private candidates' entries.</b>	Candidate name Candidate number Candidate D.O.B Candidate home address Candidate email address	In the exams office and on the exams officers computer	Limited to 4 key holders and exam officers computer is password protected.	To be stored safely and securely until after the deadline for EAR's and the resolution of any outstanding enquiry's/appeal or malpractice investigations for the exam series.
Resolving clashes information	<b>Any information relating to the resolution of a candidate's clash of exam papers or timetable variation.</b>	Candidate name Candidate number	In the exams office and on the exams officers computer	Limited to 4 key holders and exam officers computer is password protected.	To be stored safely and securely until after the deadline for EAR's and the resolution of any outstanding enquiry's/appeal or malpractice investigations for the exam series.
Results information	<b>Broadsheets of results summarising candidate final grades by subject and exam series.</b>	Candidate name Candidate number Candidate results	Exam office computer, head of centre and head of exams computer	Secure logins	7 years
Seating plans		Candidate name Candidate number	Exam office computer & hard copy in secure storage	Secure login and limited to 4 key holders	To be stored safely and securely until after the deadline for EAR's and 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 period
					outstanding enquiry's/appeal or malpractice investigations for the exam series.
Special consideration information	<b>Any hard copy information relating to a special consideration request and supporting evidence submitted to an awarding body for a candidate.</b>	Candidate name Candidate number Candidate DOB Candidate address Candidate personal and/or medical information	Securely in exams office	Limited to 4 key holders	To be stored safely and securely until after the deadline for EAR's and the resolution of any outstanding enquiry's/appeal or malpractice investigations for the exam series.
Suspected malpractice reports/outcomes	<b>Any hard copy or digital information relating to suspected malpractice investigation/report submitted to an awarding body and outcome information from the awarding body.</b>	Candidate name Candidate number	On the exams office computer and securely in the exams office	Limited to 4 key holders	To be stored safely and securely until after the deadline for EAR's and the resolution of any outstanding enquiry's/appeal or malpractice investigations for the exam series.
Transfer of credit information	<b>Any hard copy information relating to a GCE AS transfer of credit arrangement (for a legacy unitised GCE AS specification) application</b>	Candidate name Candidate number	Exams Office		To be stored safely and securely until after the deadline for EAR's and the

<b>Information type</b>	<b>Information description (where required)</b>	<b>What personal/sensitive data is/may be contained in the information</b>	<b>Where information is stored</b>	<b>How information is protected</b>	<b>Retention period</b>
	submitted to an awarding body for candidate,				resolution of any outstanding enquiry's/appeal or malpractice investigations for the exam series.
Transferred candidate information	<b>Any hard copy information relating to an application for a transferred candidate arrangement submitted to an awarding body for a candidate.</b>	Candidate name Candidate number	Exams office computer	Secure login	To be stored safely and securely until after the deadline for EAR's and the resolution of any outstanding enquiry's/appeal or malpractice investigations for the exam series.
Very late arrival reports/outcomes	<b>Any hard or digital copies of information relating to a very late arrival report submitted to an awarding body for a candidate and outcome information from the awarding body.</b>	Candidate name Candidate number	Securely in the exams office	Limited to 4 key holders	To be stored safely and securely until after the deadline for EAR's and the resolution of any outstanding enquiry's/appeal or malpractice investigations for the exam series.