Atrium Studio School General Data Protection Regulation policy (exams)

2017/18

This policy is annually reviewed to ensure compliance with current regulations

Approved/reviewed by	
Matt Messias	
Date of next review	21st May 18

Key staff involved in the General Data Protection Regulation policy

Role	Name(s)
Head of centre	**Mr Matt Messias**
Exams officer	**Mrs Carole Chesterton**
Exams officer line manager (Senior Leader)	**Mr Garry Murphy**
Data Protection Officer	**TBC**
IT manager	**Mr Richard Penhale**

Purpose of the policy

This policy details how Atrium Studio School, 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

This data may be shared via one or more of the following methods:
- ▶ hard copy
- ▶ email
- ▶ secure extranet site(s) –eAQA; OCR Interchange; Pearson Edexcel Online; TLM.
- ▶ a Management Information System (MIS) provided by 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

Atrium Studio School 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
Computers	The IT Manager maintains all back up and up grades to ensure they are run regulary.	N/a

Software/online system	Protection measure(s)
Sims	Protected passwords; use of a mix of upper/lower cases letters and numbers; changed monthly
Awarding body secure extranet site(s)	Protected passwords; use of a mix of upper/lower cases letters and numbers; changed monthly EO has to approve the creation of new user accounts and determine access rights IT Department carry out 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

IT Manager 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.

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 regularly this includes antivirus software, firewalls 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 which is available on the shared drive.

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 Mrs Mary Hodge in writing, ID will need to be confirmed on collection of the documentation. 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 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	Exams	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	Until after the deadline for EARs or the resolution of any outstanding enquiries/appeals or malpractice investigations for the exam series
Attendance registers copies	Exams	Candidate Name	Secure storage	Only authorised staff have keys	To be retained until after the deadline for EARs or until any appeal, malpractice or other results enquiry has been completed, whichever is later. [Reference ICE 6,15]
Candidates' work	Non-examination assessment work (inc. controlled assessment/coursework) returned to the centre after awarding body moderation	Candidate Name	To be stored safely and securely along with work that did not form part of the moderation sample (including materials stored electronically)	Only authorised staff have keys	Until after the deadline for EARs or the resolution of any outstanding enquiries/appeals or malpractice investigations for the exam series. [Reference GR 3, 5]
Certificates		Candidate Name	Unclaimed/uncollected certificates to be retained securely for a minimum of 12	Only authorised staff have keys	Min 12 months

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
			months from date of issue. [Reference GR 5		
Certificate destruction information	A record of unclaimed certificates that have been destroyed.	Candidate Name	To be retained for 4 years from the date of certificate destruction. [Reference GR 5]	Only authorised staff have keys	4 years
Certificate issue information		Candidate Name DOB Exam Number	Secure storage	Only authorised staff have keys	4 years
Entry information		Candidate Name DOB Exam Number	Sims and Exam Board sites	Passwords	Until after the deadline for EARs or the resolution of any outstanding enquiries/appeals or malpractice investigations for the exam series
Exam room incident logs		Candidate Name DOB Exam Number	Secure storage	Only authorised staff have keys	Until after the deadline for EARs or the resolution of any outstanding enquiries/appeals or malpractice investigations for the exam series
Post-results services: confirmation of candidate consent information		Candidate Name DOB Exam Number	Secure storage	Only authorised staff have keys	Until after the deadline for EARs or the resolution of any outstanding enquiries/appeals or malpractice investigations for the exam series
Post-results services: requests/outcome information		Candidate Name DOB Exam Number	Secure storage	Only authorised staff have keys	Until after the deadline for EARs or the resolution of any outstanding enquiries/appeals or malpractice investigations for 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
					exam series
Post-results services: scripts provided by ATS service		Candidate Name DOB Exam Number	Secure storage	Only authorised staff have keys	Until after the deadline for EARs or the resolution of any outstanding enquiries/appeals or malpractice investigations for the exam series
Post-results services: tracking logs		Candidate Name DOB Exam Number	Secure storage	Only authorised staff have keys	Until after the deadline for EARs or the resolution of any outstanding enquiries/appeals or malpractice investigations for the exam series
Resolving clashes information			Secure storage	Only authorised staff have keys	Until after the deadline for EARs or the resolution of any outstanding enquiries/appeals or malpractice investigations for the exam series
Results information		Candidate Name DOB Exam Number	Sims	Passwords	Until after the deadline for EARs or the resolution of any outstanding enquiries/appeals or malpractice investigations for the exam series
Seating plans		Candidate Name Exam Number	Secure storage	Only authorised staff have keys	Until after the deadline for EARs or the resolution of any outstanding enquiries/appeals 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
Special consideration information		Candidate Name DOB Exam Number	Secure storage	Only authorised staff have keys	Until after the deadline for EARs or the resolution of any outstanding enquiries/appeals or malpractice investigations for the exam series
Suspected malpractice reports/outcomes		Candidate Name DOB Exam Number	Secure storage	Only authorised staff have keys	Until after the deadline for EARs or the resolution of any outstanding enquiries/appeals or malpractice investigations for the exam series
Transfer of credit information		Candidate Name DOB Exam Number	Sims and Exam Board sites	Passwords	Until after the deadline for EARs or the resolution of any outstanding enquiries/appeals or malpractice investigations for the exam series
Transferred candidate information		Candidate Name DOB Exam Number	Sims and Exam Board sites	Passwords	Until after the deadline for EARs or the resolution of any outstanding enquiries/appeals or malpractice investigations for the exam series
Very late arrival reports/outcomes		Candidate Name DOB Exam Number	Secure storage Exam Boards sites	Only authorised staff have keys Passwords	To be retained until the deadline for EARs or the resolution of any outstanding enquiries/appeals for the relevant exams series. [Reference ICE 6]