HEALING
SCHOOL

A Science Academy

Healing School - A Science Academy GDPR Policy (Exams) 2018/19

This policy is reviewed annually to ensure compliance with current regulations

Author	Mrs D Barnard
Date adopted by MAT Directors	
Review Date	Autumn Term 2019
Consultations/Training	Exams Officer/Inclusion Manager, SLT & Governors

Purpose of the policy

This policy details how Healing 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
- MAT

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

- hard copy
- email
- secure extranet site(s) – e-AQA; OCR Interchange; Pearson Edexcel Online; WJEC Secure services
- The centres management Information System (MIS) provided by 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.

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

Healing School ensures that candidates are fully aware of the information and data held.

All candidates are:

- Given access to this policy via the Exams section of the school's website.
- Candidates are made aware of the above via their Exams assembly.

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	Protection measures
Desk top computer Laptop iPads	Password protection USB encryption (See AUP policy for HMAT)

Software/online system	Protection measure(s)
Sims A2C	Protected usernames and passwords; rules for password setting (use of a mix of upper/lower cases letters and numbers); users should regularly update passwords; centre administrator has to approve the creation of new user accounts and determine access rights; regular checks to Firewall/Antivirus software are carried out.

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**

The DPO 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 include:

- password protected area on the centre's intranet
- secure drive accessible only to selected staff
- regular updates undertaken (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 which is available from the Exams Officer or the O: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 the Exams office via the office email address available on the school website, or in writing. 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 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. 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 Locked in Exams office	Until expired
Attendance registers copies	Completed for each external examination	Candidate name Candidate number	Examination seating files	Locked in Exams office	1 academic year
Candidates' work	Non examined assessment	Candidate name Candidate number	Students informed to keep securely if permitted to take work away to work on Lockable cabinets within departments Secure storage in exams on return from moderator	In secure area within departments	Returned to departments after post results Students may collect the work after this time or agree for the work to be used in teaching and learning
Certificates	Candidate Results	Candidate name Candidate results by AB	Locked cabinet in school reception	Locked	1 year
Certificate issue information	Certificates distributed annually via registers All students must sign for the	Candidate name Results achieved	Locked cabinet exams office	Restricted access to locked cabinet	4 years

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
	collection of certificates				
Entry information		Candidate name Candidate number/ UCI/ ULN Gender Examination entries	Sims system Timetables issued to Candidates Mark sheets Entry lists	Password Locked storage	1 academic year
Exam room incident logs		Candidate name Candidate number Access arrangements	Exams office	Locked office; limited access	1 academic year
Overnight supervision information		Candidate name Candidate number Exam information	Electronically Hard copy: exams office	Limited access Locked office	1 academic year
Post-results services: confirmation of candidate consent information		Candidate name Candidate number Awarding board & award DOB Result	Email Awarding body website Sims system EAR file exams	Password protected Locked cabinet	1 academic year
Post-results services: requests/outcome information		Candidate name Candidate number Awarding board & award DOB Result	Email Awarding body website Sims system EAR file exams	Password protected Locked cabinet	1 academic year
Post-results services: scripts provided by ATS service		Candidate name Candidate number Awarding board & award DOB	Email Awarding body website Sims system EAR file exams	Password protected Locked cabinet	1 academic year

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
		Result			
Post-results services: tracking logs		Candidate name Candidate number Payment method Award code	Electronically EAR folder	Password protected Locked exams office	1 academic year
Resolving clashes information	Sims clash document Letters produced and sent home	Candidate name Candidate number DOB Exam award Address details	Examinations office Electronically	Locked office Password protected	1 academic year
Results information		Candidate name Candidate number/UCI/ULN DOB Results for all awards taken	Electronically	Password protected	7 years
Seating plans		Candidate name Candidate number Access arrangement	Exams office	Locked office	1 academic year
Special consideration information		Candidate name Candidate number DOB Reason for Special consideration	Exams office AB website	Locked office	1 academic year
Suspected malpractice reports/outcomes		Candidate name Candidate number Reason for report	Electronically Email	Password protected	1 academic year

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
Very late arrival reports/outcomes		Candidate name Candidate number Reason for report	Electronically Email	Password protected	1 academic year