Stone Lodge School

Stone Lodge Therapeutic School
Exams Department
Data Protection Policy

Approved by:	O Sharp	**Date:** 29/04/2026
Last reviewed on : 27.01.2026		Reviewed by: S Hilton
Next review by: Jan 27		

Purpose of the policy

This policy details how Stone Lodge Therapeutic School, in relation to exams management and administration, ensures compliance with the regulations as set out by the Data Protection Act 2018 (DPA 2018) and 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's General Regulations for Approved Centres (section 6.1) reference is made to 'data protection legislation'. This is intended to refer to UKGDPR, 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 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

To ensure that the centre meets the requirements of the DPA 2018 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 below.

Candidates' exams-related data may be shared with the following organisations:

- Awarding bodies
- Joint Council for Qualifications
- Other organisations, such as and not limited to, the Department for Education; Local Authority

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

- hard copy
- email
- secure extranet site(s) – AQA Centre Services; OCR Interchange; Pearson Edexcel Online; WJEC Secure Services
- Management Information System (MIS) provided by ESS 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

Stone Lodge Therapeutic School ensures that candidates are fully aware of the information and

data held. All candidates are:

- informed via induction booklet upon joining the school
- given access to this policy via school website, or upon request

Candidates are made aware of the above at the start of their course of study leading to an externally accredited qualification, and upon joining the school.

At this point, the centre 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 (or law relating to personal data in any jurisdiction in which the awarding body or centre are operating).

Candidates eligible for access arrangements/reasonable adjustments which require awarding body approval approval using *Access arrangements online* are also required to provide their consent by signing the GDPR compliant JCQ candidate personal data consent form before approval applications can be processed online.

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 measure(s)
Exams Officer laptop	Machine is a member of a domain and locked down using GPO. Sophos anti-virus software installed. All staff use restricted logon accounts. Swiftcomm are our IT dept.
Invigilators laptop	Machine is a member of a domain and locked down using GPO. Sophos anti-virus software installed. All staff use restricted logon accounts.

Software/online system	Protection measure(s)
Behaviourwatch	Protected usernames and passwords; rules for password setting (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.

Awarding Body Websites	Protected usernames and passwords; rules for password setting (use of a mix of upper/lower cases letters and numbers);

A2C	Protected usernames and passwords; rules for password setting (use of a mix of upper/lower cases letters and numbers); only accessible via Exams Officer's password protected PC.

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**

Ollie Sharp would report to Mohamed Damani and 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 are completed as needed in line with the manufacturer's guidelines (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/accessible from the Exams Officer and/or the staff drive.

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 Exams Officer or Data Protection Officer in writing/email. If a former candidate is unknown to current staff, they will be asked to confirm some personal information.

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 Head of Centre 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 announced, 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.

Current and former candidates can request access to the information/data held on them by making a **subject access request** to Mr O Sharp in writing; which includes email, and be addressed to the Principal. If the initial request does not clearly identify the information required, then further enquiries will be made.

The identity of the requestor must be established before the disclosure of any information, and checks should also be carried out regarding proof of relationship to the child. Evidence of identity can be established by requesting production of:

ϒ passport

ϒ driving licence

ϒ utility bills with the current address

ϒ Birth / Marriage certificate

ϒ P45/P60

ϒ credit card or mortgage statement

(This list is not exhaustive)

All requests will be dealt with within 40 calendar days. Please see Appendix 1 of the EMAT Data Protection and Data Retention Policy for further details.

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.

Sharing information with parents

We collect and hold personal information relating to our students and may also receive information about them from their previous school and forward information to a school that they are transferring to. The school processes student information within the remit of the Regulation (EU) 2016/679 (General Data Protection Regulation), referred to as the GDPR throughout this statement.

The categories of pupil information that we collect, hold and share include:

• Personal information (such as name, unique pupil number, and address)

• Characteristics (such as ethnicity, language, nationality, religion, country of birth and free school meal & PPI eligibility)

• Attendance information (such as sessions attended, number of absences and absence reasons) • Assessment information (such as internal tests, student progress information, examination results)

• Medical information (such as allergies, required medication, medical incidents that have occurred inside and outside of school that may affect learning or safety, physical or mental health needs)

• Special Educational Needs and Disabilities information (such as specific learning difficulties, medical and learning needs)

• Behavioural information (such as rewards, achievements, behaviour incidents, exclusions, detentions)

• Transport arrangements (such as bus number and route)

• First aid incidents and accident information • Post-16 information (such as destinations data, UCAS applications and grants)

• Some financial information (such as bank details for bursary applications)

Why we collect and use this information:

We use the pupil data:

• to support pupil learning

• to monitor and report on pupil progress

• to provide appropriate pastoral care and guidance

• to assess the quality of our services

• to comply with the law regarding data sharing

• to make payments to eligible students

The lawful basis on which we use this information:

We collect and use pupil information under Article 6 and Article 9 of the GDPR. This enables the school to process information such as assessments, Special Educational Needs requests, departmental censuses under the Education Act 1996 and the Education 2 Act 2005, examination results and other such data processes that relate educational data to the individual within the requirements of the school to provide education for the individual.

The centre will take into account any other legislation and guidance regarding sharing information with parents (including non-resident parents and a local authority (the 'corporate parent'), 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

  (Updated 24 August 2023 to include guidance on the role of the 'corporate parent', releasing GCSE results to a parent and notifying separated parents about a child moving school)
- School reports on pupil performance www.gov.uk/guidance/school-reports-on-pupil-performance-guide-for-headteachers

Publishing exam results

When considering publishing exam results, Stone Lodge Therapeutic School will make reference to the ICO (Information Commissioner's Office) https://ico.org.uk/your-data-matters/schools/exam-results/ Can schools give my exam results to the media for publication?

Stone Lodge Therapeutic School will publish exam results to the media or within the centre (e.g. on an honours board) in line with the following principles:

1. Refer to guidelines as published by the Joint Council for Qualifications
2. Act fairly when publishing results, and where people have concerns about their or their child's information being published, taking those concerns seriously
3. Ensure that all candidates and their parents/carers are made aware as early as possible whether examinations results will be made public and how this will be done
4. Explain how the information will be published. For example, if results will be listed alphabetically, or in grade order

As Stone Lodge Therapeutic School will have a legitimate reason for publishing examination results, consent is not required from students or their parents/carers for publication. However, if a student or their parent/carers have a specific concern about publication of their results, they have the right to object. This objection must be made in writing to Ollie Sharp, who will consider the objection before making a decision to publish and reply with a good reason to reject the objection to publish the examination results.

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	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 Secure user name and password In secure office (SENDCo)	As per school's data retention policy
Alternative site arrangements	Candidate Name Candidate DoB Gender	In secure office	In secure office (Exams Office) passcode protected	After deadline for post-results enquiries
Attendance registers copies	Candidate Name	In secure office	In secure office (Exams Office) passcode protected	After deadline for post-results enquiries
Candidates' scripts	Candidate Name	In secure office	Exams Office – passcode and security padlock protected	Collected by courier daily
Candidates' work	Candidate Name Candidate DoB Gender	In secure office	Exams Office – passcode and security padlock protected	After deadline for post-results enquiries, then handed back to subject teacher

Information type	What personal/sensitive data is/may be contained in the information	Where information is stored	How information is protected	Retention period
Centre consortium arrangements for centre assessed work	Candidate Name Candidate DoB Gender	In secure office Exams Officer's PC AAO	Secure office, passcode protected PC password protected	After deadline for post-results enquiries
Certificates	Candidate Name **Candidate DoB** **Gender**	In secure office	Exams Officer has the key to access	Minimum one year.
Certificate destruction information	Candidate Name Candidate DoB Gender	In secure office	Passcode protected office	Minimum 4 years
Certificate issue information	Candidate Name	In secure office	Passcode protected office	As per school's data retention policy
Conflicts of Interest records	Candidate Name Candidate DoB Gender Staff Member Name	In secure office Exams Officer's laptop	Passcode protected office Password protected PC	After deadline for post-results enquiries
Entry information	Candidate Name Candidate DoB Gender	In secure office Exams Officer's laptop A2C Awarding Body Websites	Passcode protected office Password protected PC Password protected websites	After deadline for post-results enquiries
Exam room incident logs	Candidate name Medical Information Safeguarding Information	In secure office Exams Officer's laptop	Passcode protected office Password protected PC	After deadline for post-results enquiries

Information type	What personal/sensitive data is/may be contained in the information	Where information is stored	How information is protected	Retention period
Invigilator and facilitator training records	Staff Member Name	In secure office Exams Officer's laptop	Passcode protected office Password protected PC	After deadline for post-results enquiries
Overnight supervision information	Candidate Name Candidate DoB Gender Candidate Address Parent/Carer Name Parent/Carer Address	In secure office Exams Officer's laptop	Passcode protected office Password protected PC	After deadline for post-results enquiries
Post-results services: confirmation of candidate consent information	Candidate Name	In secure office Exams Officer's laptop	Password protected Secure office	After deadline for post-results enquiries and certificates received
Post-results services: requests/outcome information	Candidate Name Candidate DoB Exams Results	Exams Office or Exams Officer's laptop	Password protected Secure office	After deadline for post-results enquiries and certificates received
Post-results services: scripts provided by ATS service	Candidate Name Confidential Candidate Work	Exams Office or Exams Officer's laptop	Password protected Secure office	Handed straight to the candidate or staff member that requested them. Log kept.
Post-results services: tracking logs	Candidate Name Candidate DoB	In secure office Exams Officer's laptop	In secure office (Exams Office) password protected	After deadline for post-results enquiries and certificates received

Private candidate information	Candidate Name Candidate DoB Candidate Address Access Arrangement Information	In secure office	In secure office (Exams Office) passcode protected	After deadline for post-results enquiries

Information type	What personal/sensitive data is/may be contained in the information	Where information is stored	How information is protected	Retention period
Resolving timetable clashes information	Candidate Name	In secure office	Password protected Secure office	After deadline for post-results enquiries
Results information	Candidate Name Candidate DoB Gender Results Information	Awarding body websites Email A2C	Exams Officer and SLT only have access – security password protected.	After deadline for post-results enquiries
Seating plans	Candidate Name	In secure office	In secure office (Exams Office) passcode protected	After deadline for post-results enquiries
Special consideration information	Candidate Name Medical Information Safeguarding Information	In secure office	In secure office (Exams Office) passcode protected	After deadline for post-results enquiries
Suspected malpractice reports/outcomes	Candidate Name Candidate D0B	In secure office	In secure office (Exams Office) passcode protected	After deadline for post-results enquiries
Transferred candidate arrangements	Candidate Name Candidate D0B Candidate Address	In secure office	In secure office (Exams Office) passcode protected	After deadline for post-results enquiries
Very late arrival reports/outcomes	Candidate Name Candidate DoB Medical Information	In secure office	In secure office (Exams Office) passcode protected	After deadline for post-results enquiries