	ST ALBANS GIRLS' SCHOOL
EXAMS - General Data Protection Regulation Policy	
GB sub-committee: Curriculum, Assessment & Standards Committee	
Co-ordinator: Mrs M Maddison	
Last Reviewed: Summer 2023	**Next Review: Summer 2024**
	
Signed by: **Margaret Chapman** ***Head Teacher***	**Signed by:** **Claire Barnard** ***Chair of Governors***

Purpose of the Policy
This policy details how St Albans Girls' School, in relation to exams management and administration, ensures compliance with the regulations as set out by the General Data Protection Regulation (GDPR) Data Protection Act (DPA) Act 2018 and UK 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 is operating. In these General Regulations reference is made to 'data protection legislation'. This is intended to refer to UK GDPR, the Data Protection Act 2018 and any statutory codes of practice issued by the Information Commissioner in relation to such legislation. (JCQ General Regulations for Approved Centres (section 6.1) **Personal data**) 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 exam 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 and UK 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 Officer to hold exam related information on candidates taking external examinations. For further details on the type of information held please refer to Section 5 below.

Candidates' exam related data may be shared with the following organisations/people:

- Awarding bodies
- Joint Council for Qualifications
- Department for Education
- Local Authority
- Atlas Multi Academy Trust
- School consortium
- Exam Board Moderators
- Centre staff including invigilators as necessary
- Parents of student
- UCAS
- Learning Records Service

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

- Hard copy
- USB memory sticks
- CD/DVD recordings
- Post/Parcelforce Yellow Label service
- Email
- Secure extranet sites – AQA Centre Services; OCR Interchange; Pearson Edexcel Online; WJEC Secure Services; City and Guilds; CISI Financial Qualification
- Management Information System – MIS; sending and receiving electronic data interchange using A2C from awarding body processing systems.
- Personally by telephone conversations

This data may relate to exam entries, access arrangements, the conduct of exams and non-examination assessments, special consideration requests, exam results, post result services and certificate information.

Section 2 – Informing candidates of the information held

St Albans Girls' School ensures that candidates are fully aware of the information and data held and that awarding bodies may be required to provide personal data to the agencies listed in **Section 1**.

All candidates are:

- Informed via regularly updated policies (including the JCQ document Information for candidates – Privacy Notice, General and Vocational Qualifications, which explains how the JCQ awarding bodies process their personal data in accordance with the DPA 2018 and UK GDPR), on the school website, written request and via the MIS.
- Candidates are made aware of the above in assemblies, via the school website and when qualifications are submitted to awarding bodies for processing.
- 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 is protected in line with the DPA and GDPR requirements.

Hardware	Date of Purchase & Protection Method	Warranty Expiry
Desktop Computer	Refer to IT Policy	N/A
Chromebooks		
PCs		
USB Sticks		
Software	Date of Purchase & Protection Method	Warranty Expiry
MS Office Word and Excel	Refer to IT Policy	N/A
Google Drive (Docs, Sheets, Slides)		
MIS System		
Email		
A2C (used to transfer data to Exam Boards) Information stored in a secure Exams folder. Access limited to designated staff.		
Awarding body secure websites		
Software/online systems protection measures	Date of Purchase & Protection Method	Warranty Expiry
Refer to IT Policy for further details of data security measures, including rules for password setting, regular checks to Firewall/Antivirus software.		

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 fire or flood
- Hacking attack
- 'Blagging' offences where information is obtained by deceiving the organisation who hold
- Cyber-attacks involving ransomware infections

If a data breach is identified, the following steps will be taken:

1. Containment and Recovery

Mr P O'Neil will lead on investigating the breach.

Refer to the GDPR Policy for details on how the breach will be investigated, including:

- 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.

Where malpractice is suspected or alleged, **personal data** of any person involved in administering, teaching, or completing examinations/assessments will be provided to awarding bodies, the qualifications regulator(Ofqal) or professional bodies in accordance with the *JCQ publication Suspected Malpractice – Policies and Procedures.*

4. Evaluation and Response

Once a data breach has been resolved, a full investigation of the incident will take place.
Refer to GDPR and Freedom of Information Policy for details.

The investigation will:

- Review what data is held, where and how it is stored
- Identify where risks and weak points in security measures lie (for example, use of portable storage devices or access to public networks)
- Review methods of data sharing and transmission

- Increase staff awareness of data security and filling gaps through training or tailored advice
- Review 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.

Refer to the GDPR Policy for full audit and protection measures

Section 6 – Data retention periods
Refer to Record Retention Policy

Section 7 – Access to information
Current and former candidates can request access to the information/data held on 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

A subject access request can be made to Mr P O'Neil, Chief Operations Officer, in writing/email. All requests will be dealt with within 40 calendar days. ID will need to be confirmed if a former candidate is unknown to current staff.

5. 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. The Data Protection Officer will confirm the status of these agreements and approve/reject any requests.

Sharing Information with Parents
The centre will take into account any other legislation and guidance regarding sharing information with parents (including non-resident parents), 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
- 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, St Albans Girls' 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?

Section 8 – Table recording candidate exams-related information held

Information Type	Description	What information is contained	Where is information stored	What protection	Retention Period
Exam Access Arrangement Information		Candidate name Candidate DOB Gender Data Protection Notice Candidate number UCI Diagnostic testing outcome Specialist reports that may include candidate address Personal medical information EHCP Evidence of normal way of working	JCQ Access Arrangements Online portal Legacy Exam Access arrangements files are held on site at STAGS in lockable filing cabinets which are locked and secure in the SENCo Office Current Exam Access Arrangements files are in online folders in the secure area of Google Drive and the MIS (online) MIS Lockable filing cabinet Locked and secure in SENCo Office	Secure username and password In secure area solely assigned to exams	Until the student is 25 years of age
Attendance Registers copies			Secure Exams Office		Exam Series

Candidates' work	MFL orals are stored in the secure area of the MIS and uploaded to the awarding bodies secure portals via digital submission	Candidate Number Name	Secure area of MIS	Secure username and password	Exam Series
Certificates	Hard copy Exam Board Certificates	Candidate number Candidate name Exams taken Exam results	Secure Exams Office		Obligatory period 1 year but keep for 2 years. A record of certificates that have been destroyed is kept for 4 years
Conflict of Interest Records	Hard Copy, Google Drive	Name Relationship	Exams Office		Exams series
Certificate Issue information		Name House Signatures Date of collection	Excel and Secure Exams Office		Exam Series
Exam room incident logs		Date Time Exam Invigilator names Access arrangements	Secure Exams Office		Exam Series

		Record of any incidents during exam – can include personal candidate details for instance illness.			
Overnight Supervision Information	Hard Copy	Name	Secure Exams Office		Exam Series
Post Results information		EAR forms with candidate number, name, email and phone number details	Secure Exams Office Secure username and password.		Hard copy maintained for 2 years
Post result service scripts			Stored on line in secured area		Exam series
Private Candidate information		Candidate name, address, DOB, passport and/or driving licence details	Secure Exams Office On Line	Secure username and password	Exam series
Resolving clash candidate information		Exam details, times and candidates' names	Excel	Secure username and password	Exam series
Result information		Candidate name, candidate number exams taken and outcomes	MIS	Secure username and password	Until student is deleted from MIS system
Seating plans		Candidate name Candidate number Access candidates highlighted	Exam Hall Secure Exams office		Exam series
Special consideration information		Candidate name, Candidate number Personal information pertinent to request Medical evidence	Secure Exams Office	Secure Exam Board Sites Secure username and password protected folder	Exam series

				Hard copy in secure office	
Suspected malpractice reports and outcomes		Candidate name Candidate number Evidence	Secure Exams Office Online	Secure username and password Exam Board website	Exam series

For details of how to request access to information held, refer to section 7 of the **Access to Information Policy**

For further details of how long information is held, refer to section 6 of the **Data Retention Periods Policy**