GDPR (Exams) Policy

Contents

Key staff involved in GDPR (Exams) Policy

Role	Name(s)
Head of Centre	Jason Davis
Data Protection Co-ordinator	Joanne Bruton
Exams Manager	Simone Noel
Business Manager	David James
SLT Member(s)	David Harris
IT Manager	Luke Shears

Approved: Governing Body
Approved: March 2020

Review completed January 2022
Review due January 2023

Member of staff with Lead Responsibility for this policy: Mrs S Noel (Exams Manager)

Purpose of the policy

This policy details how Sturminster Newton High 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
- Department for Education; Local Authority
- Schools / colleges that the students attend after leaving us
- The School Governors
- Youth support service
- Careers Advisors
- Post 16 Education & Training Providers

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

- Hard copy
- Email – Password protected
- Secure extranet site(s) e-AQA; OCR Interchange; Pearson Edexcel Online;
- 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

Sturminster Newton High School ensures that candidates are fully aware of the information and data held.

All candidates are:

- Informed via electronic communication and the website.
- Given access to this policy via Sturminster Newton High School website, a hard copy can be requested from the school office.
- Privacy notice as they join the school.

Candidates are made aware of the above at the start of their course of study leading to external examinations.

The centre also brings to the attention of candidates the annually updated JCQ document Information for Candidates – Please refer to Privacy Notice DOC100 V1 which explains how the JCQ awarding bodies process their personal data in accordance with the DPA 2018 and GDPR

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
School Network – Desktop Computer	Various purchase dates Hardware is checked on a weekly basis to ensure it is running. Anti-virus is cloud hosted and updates are applied automatically each day. Students and staff have individual logins to the network and permissions are allocated depending on the users groups.	All out of warranty
School Network – Laptop	May 2018 Hardware is checked on a weekly basis to ensure it is running. Anti-virus is cloud hosted and updates are applied automatically each day. Students and staff have individual logins to the network and permissions are allocated depending on the users groups. School owned laptops connect to their own SSID	
Admin Network – Desktop Computer	June 2019 Hardware is checked on a weekly basis to ensure it is running. Anti-virus is cloud hosted and updates are applied automatically each day. Students and staff have individual logins to the network and permissions	

	are allocated depending on the users groups. Access to secure admin area only available from Admin PCs.	

Software/online system	Protection measure(s)
School Server:	Servers are kept in a secure location restricted to authorised staff. Logins for the servers are protected by passwords
Admin Network:	Same as school server – all machines on one network
MIS (SiMS)	Access level determined by permission level (as set by Head of Centre) Usernames are protected by passwords
Awarding Body Secure Extranets: AQA OCR Pearson Edexcel	Exam Manager manages account permissions for the school Unique usernames protected by personal passwords
A2C	Installed only on Exam Manager's computer
FFT Aspire	Unique usernames protected by personal passwords

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.

(Please refer to Data Breach Procedure DOC106 V1)

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

The data protection team Joanne Bruton, Luke Shears and David James must be contacted immediately once the breach has been identified, by e-mail or GDPRis or by the data mandate form – please refer to the data breach procedure for further information.

1. Containment and recovery

Joanne Bruton (Data Protection Co-ordinator) 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.
- 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 twice a year.

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 day – Antivirus (updated every day, scanned daily)
- Windows updates (as provided by Microsoft)

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 destruction checklist which is available/accessible from the data protection team. A hard copy is kept in the Exams Office.

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 Jason Davis (Head of Centre). At the point of request, the person requesting data will be issued with a Data Subject Access Request form, explaining the process and their rights as a data subject. 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.

The school will, in general, only disclose data about individuals with their consent. However, there are circumstances under which the schools authorised officer may need to disclose data without explicit consent for that occasion.

These circumstances are strictly limited to:

- Student data disclosed to authorised recipients related to education and administrators necessary for the school to perform its satisfactory duties and obligations.
- Students data disclosed to authorized recipients in respect of the child's health, safety and welfare.
- Student data disclosed to parents in respect of their child's progress, achievements, attendance, attitude or general demeanor within or in the vicinity of the school.
- Unavoidable disclosures, for example to an engineer during maintenance of the computer system. In such circumstances, the engineer would be subject to a confidentiality clause. Personnel working on behalf of the LA are contractually bound not to disclose personal data.
- The school must ensure that any 'third party' contractors handling data sign an undertaking to abide by the principles of the GDPR (2018).

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.

To be read in conjunction with:

- Privacy Notice DOC100 V1
- Data Breach Procedure DOC106 V1

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, 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 (SiMS) Exams secure storage SEN secure storage	Secure name and password protected Secure storage has authorised key holder(s)	DOB of the candidate + 25 years (ARSR&SDD)
Attendance registers copies	Candidate Name, Number Candidate Tier Information (if applicable)	Exams secure storage	Secure storage solely assigned to exams	Until certification (JCQ ICE 22.5)
Candidates' scripts	Candidate Name, Number Candidate Tier Information Candidate Assessment Data	Exams secure storage Staff room Classrooms	Secure storage solely assigned to exams Staffroom only staff permitted by electronic entry Lockable filing cabinets in classrooms or designated department storage	Unwanted scripts securely destroyed
Candidates' work	Candidate Name, Number, Tier Information	NEA returned to subject teachers, securely stored until certification	Lockable filing cabinets in classrooms or designated department storage	Returned to candidate or securely destroyed after certification
Certificates	Candidate Name, DOB Qualification Grades	Exams secure storage Front Office	Secure storage solely assigned to exams Lockable cupboard	Return to Awarding Body or securely destroy 12 months from date of issue (JCQ GR 5.14)

Information type	What personal/sensitive data is/may be contained in the information	Where information is stored	How information is protected	Retention period
Certificate destruction information	Candidate Name, DOB Qualification Grades	Exams secure storage	Secure storage solely assigned to exams	A record of certificates destroyed retained for a period of 4 years from date of destruction (JCQ GR 5.14)
Certificate issue information	Candidate Name, Number	Exams secure storage	Secure storage solely assigned to exams	Minimum of 12 months (JCQ GR 5.14)
Entry information	Candidate Name, Number, Tier	MIS (SiMS)	Secure username and password protected	Hard copies securely destroyed after certification
Exam room incident logs	Candidate Name Candidate Number Details of incident involving candidate(s)	Exams secure storage	Secure storage solely assigned to exams	Securely destroyed after certification
Overnight supervision information	Candidate Name, Number Candidate Contact Details Details of Overnight Supervision Arrangement	Exams secure storage	Secure storage solely assigned to exams	Securely destroyed after certification
Invigilator training records	Invigilator Name	Exams secure storage	Secure storage solely assigned to exams	Until certification of each exam series (JCQ ICE 12)
Post-results services: confirmation of candidate consent information	Candidate Name, Number Qualification Grades and Marks	Exams secure storage	Secure storage solely assigned to exams	Forms retained for 6 months from date of given consent, then securely destroyed (PRS 4.2.1)
Post-results services: requests/outcome information	Candidate Name, Number Qualification Grades and Marks	Exams secure storage	Secure storage solely assigned to exams	Unwanted information securely destroyed after certification
Post-results services: scripts provided by ATS service	Candidate Name, Number Qualification Grades and Marks Candidate Script	Exams secure storage Staff room Classrooms	Secure storage solely assigned to exams Staffroom only staff permitted by electronic entry Lockable filing cabinets in classrooms or designated department storage	Unwanted scripts securely destroyed
Post-results services: tracking logs	Candidate Name Candidate Number	Secure folder	Secure username and password protected	Until certification

Information type	What personal/sensitive data is/may be contained in the information	Where information is stored	How information is protected	Retention period
Private candidate information	Candidate Name, Number Address, Photocopy of proof of identity	Exams secure storage	Secure storage solely assigned to exams	Securely destroyed after certification
Resolving clashes information	Candidate Name, Number Candidate Tier Information (if applicable)	Secure folder	Secure username and password protected	Until certification
Results information	Candidate Name, Number Candidate Tier Information Qualification Grades and Marks	MIS (SiMS) Secure storage	Secure username and password protected Secure storage has authorised key holder(s)	DOB of the candidate + 25 years (ARSR&SDD 5.1.2) Hard copies securely destroyed after certification
Seating plans	Candidate Name, Number	MIS (SiMS)	Secure username and password protected	Hard copies securely destroyed after certification
Special consideration information	Candidate Name, Number, DOB, UCI, Qualification codes Medical or mental health details	Awarding body extranet site Secure storage	Secure username and password protected Secure storage has authorised key holder(s)	Hard copies securely destroyed after certification
Suspected malpractice reports/outcomes	Candidate Name, Number, DOB, UCI Qualification codes Personal details pertaining to suspected malpractice	Secure folder Awarding body Secure storage	Secure username and password protected Secure storage has authorised key holder(s)	Hard copies securely destroyed after certification
Transfer of credit information	Candidate Name, Number, UCI	Secure folder Awarding body extranet site Previous school	Secure username and password protected	Hard copies securely destroyed after certification
Transferred candidate information	Candidate Name, Number, UCI Candidate Tier Information (if applicable)	Secure folder Awarding body extranet site Previous school	Secure username and password protected	Hard copies securely destroyed after certification
Very late arrival reports/outcomes	Candidate Name, Number Qualification Codes Personal details pertaining to lateness	Awarding body extranet site Secure storage	Secure username and password protected Secure storage has authorised key holder(s)	Hard copies securely destroyed after certification