Blessed George Napier RC School

General Data Protection Regulation policy (Exams)

2023/24

This policy is annually reviewed to ensure compliance with current regulations

Approved/reviewed by	
Date of next review	October 2024

Purpose of the policy

This policy details how Blessed George Napier 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 UK General Data Protection Regulation (GDPR) and should be read alongside the school's Data Protection Policy and the Subject Access Request Policy.

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 UK GDPR, 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 UK GDPR, all candidates' exam information – even that which is not classified as personal or sensitive – is covered under this policy.

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
- Multi Academy Trust
- Local Authority
- The Press

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

- hard copy
- email
- secure extranet site(s) i.e., AQA Centre Services; OCR Interchange; Pearson Edexcel Online; WJEC Secure Website, JCQ CAP
- Management Information System (MIS) provided by Capita SIMS.

- Sending/receiving information via electronic data interchange (EDI) using 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, malpractice, special consideration requests and exam results/post-results/certificate information.

Informing candidates of the information held

Blessed George Napier School ensures that candidates are fully aware of the information and data held.

All candidates are:

- Directed to the GDPR Exam related specific policy via the Exam Information Booklet
- Given access to this policy via centre website

Candidates are made aware of the above when Information booklets are distributed at the point that entries are made, this will include the JCQ Privacy notice.

Candidates eligible for access arrangements/reasonable adjustments which require awarding body 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.

Hardware & Software

IT hardware, software and access to online systems is protected in line with GDPR UK requirements and is detailed in the school's GDPR policy.

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**

Mrs A Robey (Data Protection Officer) 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

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

Data retention periods

Details of retention periods, the actions taken at the end of the retention period are detailed at the end of this policy. Hard copy records are shredded.

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 results, 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

Current and former candidates can request access to the information/data held on them by making a **subject access request** to the Data Protection Officer in writing/email. ID will need to be confirmed if a former candidate is unknown to current staff before request are actioned. All requests will be dealt with within one month in line with the school's Subject Access Request Policy available from the school website.

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 exam results have been published, 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.

Third party access

Written permission must 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

All external exam information will be sent via candidates. Information regarding results will only be given to parents/third parties on receipt of written authorisation from the candidate in line with the school's Subject Access Request Policy

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	Application information	Candidate name Candidate DOB Gender Data protection notice – could include - candidate signature, parental signature, name candidate number, home address. Diagnostic testing outcome(s) Specialist report(s) outlining specific difficulties (may also include candidate address) Evidence of normal way of working	Access Arrangements Online MIS Lockable metal filing cabinet	Secure username and password In secure area solely assigned to exams Within SEN dept and Exams office	7 years
Attendance registers copies	Exam/Mock registers	Name, candidate number	Exams Office	Locked Office	1 year max
Candidates' scripts	Word processed scripts only	Name, candidate number	Electronically	In secure area solely accessible to exams officer	2 years
Candidates' work	NEA samples	Name, candidate number	Securely stored within depts. A sample will be sent to moderators, then securely stored until after ROR then returned to department to be returned to candidates or destroyed	Lockable cabinet	Until after ROR deadline

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
Certificates	External exam certificates	Name, DOB, UCI number candidate number, gender	Locked Office	Locked room until handed to candidates	Indefinitely
Certificate destruction information	.	Name, DOB, UCI number candidate number, gender	Locked Office	Locked office	Certificates are securely stored indefinitely as there are often requests for old certificates
Certificate issue information	Letter sent to leavers	Name & address	Not stored	N/A	N/A
Conflict of Interest Records	Names	Name, exam entry information	Locked Office or passed to AB via secure access	Locked office	2 Years
Entry information	Entry lists for each subject, hard copy & electronically	Name, DOB, candidate number, UCI	Locked office Electronically Sent to exam boards	Locked office Password protected Via A2C	7 years
Exam room incident logs	Record of events during exam	Name, candidate number record of incident	With the attendance registers	Stored in locked room	Until after the ROR's – 1year max
Invigilator and facilitator training records	JCQ required training, safeguarding, prevent	Name, email	TEO, hard copy file, HR office/Exams Office	Stored in locked cabinet/room	Period of service
Post-results services: confirmation of candidate consent information	Confirmation of request for ROR	Name, candidate number, email address	Hard copy Electronically	Locked Office Password protected	7 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
Post-results services: requests/outcome information	Applications from candidates	Name, candidate number, UCI, email address	Hard Copy Electronically	Stored in lockable cabinet in locked office Sent via exam board secure websites Stored on password protected files	7 years
Post-results services: scripts provided by ATS service	Applications from candidates and copies of scripts either hard copy or electronic	Name, candidate number candidates work	Hard copy Electronic copy	Hard copies are stored in lockable cabinet in a locked office Stored in a password protected file	7 years
Post-results services: tracking logs	Spreadsheet of ROR and outcomes	Name, candidate number	Electronically	Password protected file	Indefinite
Results information	External/internal exams	Name, DOB, UCI	Electronically Hard copy	Password protected Via secure exam board websites MIS system	Indefinitely
Seating plans	External/internal exams	Name, candidate number. Any incident taken place during exam	Exams Office	Locked office	Until after ROR
Special consideration information	Applications to Exam boards	Could include – name, DOB, medical, details of the circumstances surrounding the application	Exams Office Sent to exam boards	Lockable cabinet in locked office	7 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
				Sent via exam board secure website	
Suspected malpractice reports/outcomes	Applications to exam boards	Could include, name, DOB, candidate number, UCI with details of the incident causing the application	Exams Office	Lockable cabinet in locked office	7 years
Transferred candidate arrangements	Applications to boards	Name, DOB, UCI	Sent to Exam boards Hard copies stored in Exams Office	Sent via secure exam board website Stored in lockable cabinet in locked office	2 years
Very late arrival reports/outcomes	Correspondence between exam board and centre	Name, candidate number, UCI record of incident and outcome	Exams Office	Lockable cabinet in locked office	2 years