Belfast Boys' Model School

Data Protection & GDPR Policy

For Exams Management and Administration

Policy Details

Summary of Policy	The policy outlines data that is required to be kept for exam administrative purposes & how a data breach would be dealt with
Purpose	To ensure compliance with the regulations as set out by the DPA (2018) and GDPR
Operational Date	September 2024
Review Date	November 2025
Date last reviewed & approved by Board of Governors.	

Purpose of the policy

This policy details how Belfast Boys' Model 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).

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 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 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 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
- EA

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

- hard copy
- email
- secure extranet site(s) - eAQA; OCR Interchange; Pearson Edexcel Online; WJEC Secure services; OCN Quartz
- Capita SIMS sending/receiving information via electronic data interchange (EDI) using A2C

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

Section 2 – Informing Candidates

Belfast Boys' Model School ensures that candidates are fully aware of the information and data held. All candidates are:

- informed via parental information events
- given access to this policy on request

Candidates are made aware of the above at the start of their course of study leading to an externally accredited qualification. 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 GDPR. Candidates eligible for access arrangements 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 DPA & GDPR requirements.

Hardware	Protection measures	Warranty expiry
Computer in Exams Office	Protection Software and Back Up to School Server.	Renewed at end of term

Software/online system	Protection measure(s)
SIMS	Encrypted
A2C	Encrypted

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:

(i) Containment and recovery

Vice-Principal 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

(ii) 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?

(iii) 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.

(iv) 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.
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 (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 Retention policy, which is available centrally.

Section 7 – Access to information
With reference to ICO information https://ico.org.uk/for-the-public/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. (These can be requested during post-results service.)

Requesting exam information
Requests for exam information can be made to the GDPR Officer in writing. Identification of the individual will be requested to allow for information to be made available. This will include personal details retained by the school.
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.

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.

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

The centre will take into account any other legislation and guidance regarding sharing information with parents (including non-resident parents).

Section 8 – Verifying Pupil Identity

Internal Candidates

In Belfast Boys' Model School, numerous external exams are invigilated by non-teaching staff who are employed by CCEA.

At the start of each external exam the following people will be present to verify candidate identity.

They are:

1. Exams Manager
2. Curriculum Vice-Principal (or a member of SLT in their absence)
3. Head of Year/Counsellor for the cohort of pupils sitting the exam that session

The subject teacher may be present outside the exam hall and can also confirm identity.

The Form Tutor of each class may also be present outside the exam hall.

All pupils will have received an individual exam timetable to confirm the dates of their exams.

Persons 2 and 3 work closely with these pupils and are in the position to identify their identity.

Pupils are invited into the exam room individually by name by the Year Team leaders.

External Candidates

A copy of photographic evidence (and an additional form of identification) will be requested by the Examination Manager when entries are made.

All External Candidates must present this photographic ID on the day of their exam to confirm their identity.

Related Documents

1: Management of Non-Examined Assessment policy
2: Malpractice policy
3: Equality policy
4: Appeals policy
5: JCQ ICE document