Bolton Impact Trust Data Protection Policy (Exams)

Reviewed By	**Andrea Whitehead**
Last Reviewed	**September 2020**
Reviewed	**September 2021**
To be reviewed	**September 2022**

Key Staff involved in the policy

Academy Leads

Senior Leadership Team

Exam Officers

IT Support

Purpose of the policy

This policy details how Bolton Impact Trust, 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).

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 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 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.

Section 1 – Exams-related information

There is a requirement for the exams officer 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
- Department for Education; Local Authority; Multi Academy Trust.

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 Website; City & Guilds Walled Garden
- a 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; etc.

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

Bolton Impact Trust ensures that candidates are fully aware of the information and data held.

All candidates are:

- given access to this policy via the trust website

Candidates are made aware of the above at the start of a course leading to a vocational qualification, or, where candidates are following GCSE qualifications, when the entries are submitted to awarding bodies for processing.

At this point, Bolton Impact Trust 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 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 DPA & GDPR requirements.

Hardware	Date of purchase and protection measures	Warranty expiry
Desktop computer; Laptop/tablet	Hardware is checked by SICT Antivirus is updated by SICT	N/A

Software/online system	Protection measure(s)

MIS - SIMS	Protected usernames and password centre administrator has to approve the creation of new user accounts and determine access rights Regular software updates
Intranet; Internet browser(s);	Regular checks to Firewall/Antivirus software; etc.
Awarding body secure extranet site	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
A2C	Protected usernames and password to log on to the computer Only accessed on

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

The Senior Leadership Team 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 (detail the regularity).

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 3 months (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 website.

Section 7 – Access to information

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 [insert staff name and/or role e.g. the Data Protection Officer] in [insert how e.g. writing/email and how ID will need to be confirmed if a former candidate is unknown to current staff].

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

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

Bolton Impact Trust 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, Bolton Impact Trust will make reference to the ICO (Information Commissioner's Office https://ico.org.uk/your-data-matters/schools/exam-results

Publishing examination results is a common and accepted practice. Many students enjoy seeing their name in print, particularly in the local press and the GDPR does not stop this happening. However, under the GDPR schools have to act fairly when publishing results, and where people have concerns about their or their child's information being published, schools must take those concerns seriously.

Bolton Impact Trust will make sure that all pupils and their parents or guardians are aware as early as possible whether examinations results will be made public and how this will be done.

Bolton Impact Trust 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 parents/carers have a specific concern about publication of their results, they have the right to object. This objection must be made in writing to the Academy Lead, who will consider the objection before making a decision to publish and reply with a good reason to reject the objection to publish the exam 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	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		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 Educational, Health Care Plan (EHCP)	Access Arrangements Online MIS Lockable metal filing cabinet	Secure user name and pas sword In secure area solely assigned to exams	Until the expiry date has passed
Attendance registers copies		Candidate name Candidate number	Lockable metal filing cabinet	In secure area solely assigned to exams	Until the deadline for reviews of marking has passed, or any appeal, malpractice or other results has been completed, whichever is later.
Candidates' scripts	Any unwanted copies of scripts returned to the centre through the Access to Scripts (ATS) service.	Candidate name Candidate number	Lockable room	Kept in a lockable cupboard	To be retained securely until the awarding body's earliest date for confidential disposal of unwanted scripts.

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
Candidates' work	Non-examination assessment work returned to the centre by the awarding body at the end of the moderation period.	Candidate name Candidate number	To be stored safely and securely	To be stored safely and securely along with work that did not form part of the moderation sample (including materials stored electronically)	*Until the deadline for a review of moderation has passed or until a review of moderation, an appeal or a malpractice investigation has been completed, whichever is later*
Certificates	Candidate certificates issued by awarding bodies.	Candidate name Candidate DOB **Candidate results**	A lockable room	In secure area solely assigned to exams	*…retain all unclaimed certificates under secure conditions for a minimum of 12 months from the date of issue*
Certificate destruction information	A record of unclaimed certificates that have been destroyed.	Candidate name Candidate DOB **Candidate results**	A lockable room	Lockable metal filing cabinet	*…destroy any unclaimed certificates after retaining them for a minimum of 12 months. They must be destroyed in a confidential manner. Centres that do not have a means of destroying certificates confidentially may return them*

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
					to the respective awarding body.
Certificate issue information	A record of certificates that have been issued.	Candidate name Candidate DOB	In secure area solely assigned to exams	**Lockable metal filing cabinet**	*Retain them for a minimum of 12 months.*
Entry information		Candidate name Candidate DOB	Exam board Online MIS Lockable metal filing cabinet	Secure user name and password In secure area solely assigned to exams	To be retained until Results day
Exam room incident logs	**Logs recording any incidents or irregularities in exam rooms for each exam session.**	Candidate name Candidate DOB Description of incident Staff names	In secure area solely assigned to exams	**Lockable metal filing cabinet**	To be retained until the deadline for EARs or the resolution of any outstanding enquiries/appeals for the relevant exams series.
Invigilator and facilitator training records		Staff names	The exam office online In secure area solely assigned to exams	Secure user name and password In secure area solely assigned to exams	*A record of the content of the training given to invigilators must be retained on file until the deadline for reviews of marking has passed or until any appeal, malpractice or other results enquiry has been*

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
					completed, whichever is later.
Overnight supervision information	JCQ form *Timetable variation and confidentiality declaration for overnight supervision* for any candidate eligible for these arrangements.	Candidate name Candidate DOB	In secure area solely assigned to exams	**Lockable metal filing cabinet**	*Keep for inspection all completed forms available in your centre until the deadline for reviews of marking has passed or until any appeal, malpractice or other results enquiry has been completed, whichever is later.*
Post-results services: confirmation of candidate consent information	Hard copy or email record of required candidate consent	Candidate name Candidate DOB Candidate signature Candidate email address	Exam boards Online MIS In secure area solely assigned to exams	Secure user name and password Lockable metal filing cabinet	*Consent forms or e-mails from candidates must be retained by the centre and kept for at least six months following the outcome of the clerical re-check or review of marking or any subsequent appeal.*

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	Any hard copy information relating to a post-results service request (RoRs, appeals, ATS) submitted to an awarding body for a candidate and outcome information from the awarding body.	Candidate name Candidate DOB Candidate UCI number Candidate ULN number Candidate gender Candidate results	Exam boards Online In secure area solely assigned to exams	Secure user name and password Lockable metal filing cabinet	EAR consent to be retained for at least six months following the outcome of the enquiry or any subsequent appeal. ATS consent to be retained for at least six months from the date consent given.
Resolving timetable clashes information	Any hard copy information relating to the resolution of a candidate's clash of timetabled exam papers	Candidate name Candidate DOB Candidate UCI number Candidate ULN number Candidate gender	MIS In secure area solely assigned to exams	Secure user name and password Lockable metal filing cabinet	
Results information	Broadsheets of results summarising candidate final grades by subject by exam series.	Candidate name Candidate DOB Candidate UCI number Candidate ULN number Candidate gender Candidate results	Exam boards Online MIS In secure area solely assigned to exams	Secure user name and password Lockable metal filing cabinet	Records for current year plus previous 6 years to be retained as a minimum.
Seating plans	Plans showing the seating arrangements of all candidates for every exam taken.	Candidate name Staff name	In secure area solely assigned to exams	Lockable metal filing cabinet	*Until the deadline for reviews of marking has passed or until any appeal, malpractice or other results*

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
					enquiry has been completed, whichever is later.
Special consideration information	Any hard copy information relating to a special consideration request and supporting evidence submitted to an awarding body for a candidate.	Candidate name Candidate DOB Candidate UCI number Information why special consideration is needed	Exam boards Online	Secure user name and password	*The centre must retain evidence supporting an on-line special consideration application until after the publication of results*
Suspected malpractice reports/outcomes	Any hard copy information relating to a suspected or actual malpractice investigation/report submitted to an awarding body and outcome information from the awarding body.	Candidate name Candidate DOB Candidate UCI number Information why a suspected malpractice was suspected Outcome of malpractice	Exam boards Online In secure area solely assigned to exams	Secure user name and password Lockable metal filing cabinet	To be retained until the deadline for EARs or the resolution of any outstanding enquiries/appeals for the relevant exams series.
Transferred candidate arrangements	Any hard copy information relating to a transferred candidate arrangement. Applications submitted online via CAP.	Candidate name Candidate DOB Candidate UCI number Gender	Exam boards Online MIS In secure area solely assigned to exams	Secure user name and password Lockable metal filing cabinet	To be retained until the deadline for EARs or the resolution of any outstanding enquiries/appeals for the relevant exams series.
Very late arrival reports/outcomes	Any hard copy information relating to a candidate arriving very late to an	Candidate name Candidate DOB	Online via CAP Lockable metal filing cabinet	Secure user name and password	To be retained until the deadline for EARs or the

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
	exam. Reports submitted online via CAP.	Candidate UCI number			resolution of any outstanding enquiries/appeals for the relevant exams series.