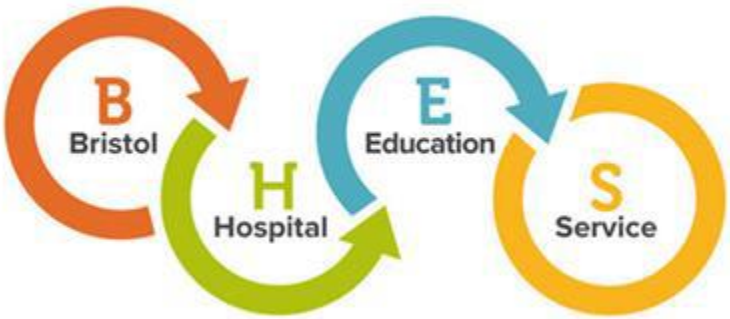

Data Protection Policy (Exams)

2020/21

This policy is reviewed annually to ensure compliance with current regulations

Approved/reviewed by	
Jim Bowyer	
Date of next review	September 2021

Key staff involved in the policy

Role	Name(s)
Head of centre	**Jim Bowyer**
Exams officer	**Claire Kitchen**
Senior leader(s)	**Sylvia Aldrich, Philippa Scholar, Gwen Bennion**
IT manager	**TWS IT**

Purpose of the policy

This policy details how [insert centre name], 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).

> At the date of reviewing these regulations, although the UK has left the European Union the General Data Protection Regulation still has a direct effect within the UK (JCQ's General Regulations for Approved Centres (GR, 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
- 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 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 – Candidate information, audit and protection measures*.

Candidates' exams-related data may be shared with the following organisations:

- Awarding bodies
- Joint Council for Qualifications (JCQ)
- [insert (by listing) any other organisations as relevant to your centre e.g. Department for Education; Local Authority; Multi Academy Trust; Consortium; the Press; etc.]

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

- hard copy
- email
- secure extranet site(s) – [insert as appropriate to your centre e.g. eAQA; OCR Interchange; Pearson Edexcel Online; WJEC Secure Website; City & Guilds Walled Garden; etc.]
- [insert any other methods as appropriate to your centre e.g. a Management Information System (MIS) provided by [insert MIS provider detail (e.g. 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

Bristol Hospital Education Service ensures that candidates are fully aware of the information and data held.

All candidates are:

- informed via electronic communication and website
- given access to this policy vis website

Candidates are made aware of the above in assemblies and via the website.

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	Date of purchase and protection measures	Warranty expiry
Desktop Computer Chrome books PC's, laptops	See BHES Inventory	Request details from TWS IT

Software/online system	Protection measure(s)
MS Office Word and Excel	Information stored in secure Exams folder.
MIS system,	Access limited to designated staff.
Email	Access limited to designated staff.
A2C (used to transfer data to Exam Boards)	Password protected
SIMS Exam Organiser	Password Protected
Awarding body secure websites	Password Protected

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:

1. **Containment and recovery**

Jim Bowyer 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.

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 Bristol Hospital Education's Exams archiving policy which is available/accessible from school website.

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 Mr Jim Bowyer in writing/email. 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.

Candidates' personal data will not be shared with a third party [insert your centre's process for sharing data with a third-party e.g. 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), 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 – can this section be deleted?

[Insert here any information or centre policy regarding publishing exam results (where applicable). Examples provided below. Where not considered relevant to include in your centre policy here, delete this table and the heading above it]

When considering publishing exam results, [insert centre name] will make reference to the ICO (Information Commissioner's Office) Schools, universities and colleges information https://ico.org.uk/your-data-matters/schools/ on Publishing 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.

Schools should 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. Schools should also explain how the information will be published. For example, if results will be listed alphabetically, or in grade order.

In general, because a school has a legitimate reason for publishing examination results, pupils or their parents or guardians do not need to give their consent to publication. However, if you have a specific concern about publication of your results, you have the right to object. Schools should consider objections from pupils and parents before making a decision to publish. A school would need to have a good reason to reject someone's objection to publication of their exam results.)

OR

[Insert centre name] will publish exam results to the media or within the centre (e.g. on an honours board) in line with the following principles:

- Refer to guidelines as published by the Joint Council for Qualifications
- Act fairly when publishing results, and where people have concerns about their or their child's information being published, taking those concerns seriously
- Ensure that all candidates and their parents/carers are aware as early as possible whether examinations results will be made public and how this will be done

- Explain how the information will be published. For example, if results will be listed alphabetically, or in grade order

As [insert centre name] will have a legitimate reason for publishing examination results, consent is not required from students or their parents or guardians for publication. However, if a student or their parents or guardians have a specific concern about publication of their results, they have the right to object. This objection must be made in writing to [insert name/role of individual], 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 number UCI Diagnostic testing outcome Specialist reports that may include candidate address Personal medical information EHCP Evidence of normal way of working	Access arrangements (on line) MIS Lockable filing cabinet Locked and secure in Exams Office	Secure username and password In secure area solely assigned to exams	Until the student is 25 years of age
Alternative site arrangements			Secure Exams Office		Exam Series
Attendance registers copies			Secure Exams Office		Exam Series
Candidates' scripts			Kept in secure Exams office until collected by Royal mail yellow label service		
Candidates work	Hard Copy Controlled assessment MFL orals on CD	Candidate number Candidate name	Secure departmental storage		Exam Series
Certificates	Hard Copy Exam board Ceritifcates	Candidate number	Secure Exams Office		Keep for 3 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
		Candidate name Exams taken Exam result			Record kept of certificates destroyed