General Data Protection Regulation policy (exams)

2019/20

This policy is reviewed annually to ensure compliance with current regulations

Approved/reviewed by	
Mrs Norris-Wright	
Date of next review	March 2020

Key staff involved in the policy

Role	Name(s)
Head of centre	**Mrs Norris-Wright**
Exams officer	**Mrs Phillips**
Exams officer line manager (Senior leader)	**Mrs Norris-Wright**
IT manager	**Mr Duckling**
Data manager	**Mrs Applegate**

Purpose of the policy

This policy details how Bexhill Academy, 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 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 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
- [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) –e.g. eAQA; OCR Interchange; Pearson Edexcel Online; WJEC Secure services; City & Guilds Walled Garden; etc.
- 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

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

Bexhill Academy ensures that candidates are fully aware of the information and data held.

All candidates are:

- given access to this policy via centre website, written request at the start of each academic year

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
[List the hardware used to manage/administer candidate information. Insert each as a new row in the table. Examples might include: Desktop computer; Laptop/tablet; etc.]	[Insert purchase date] [Insert protection measures (liaise with the IT manager to determine these). Examples might include: when hardware is checked; by who; what is checked (hard drive scans etc.); antivirus protection up to date; etc.]	[Include if applicable or indicate N/A]
Desktop computer	6/2016	
Desktop computer	6/2016	

Software/online system	Protection measure(s)
[Insert details of any software or system used where candidate information is stored]	[Insert the measures in place to protect the information from unauthorised/unlawful access (liaise with the IT/Data manager to determine these)]
[Insert each as a new row in the table. Examples might include: MIS; Intranet; Internet browser(s); Awarding body secure extranet site(s); A2C; etc.]	[Example measures might include: 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; regular checks to Firewall/Antivirus software; etc.]
MIS	Restricted users access in MIS
File Server	Strong passwords. Restricted file access permissions. A/V updated daily and monitored centrally. All access changes through IT department.
A2C	Restricted username/password

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**

Trudy Hillman (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

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 annually.

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 weekly (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 in hard copy in the file marked 'policies' above the Exams Officer's desk and is available on the Academy 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 Trudy Hillman, the Data Protection Officer 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 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

When considering publishing exam results, the centre will make reference to the ICO (Information Commissioner's Office) Education and Families https://ico.org.uk/for-organisations/education/ information on Publishing 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	Access Arrangements Online MIS Lockable metal filing cabinet	Secure user name and password In secure office (SENCo)	**6 Years**
Alternative site arrangements		Candidate name Candidate DOB Gender	MIS Lockable metal filing cabinet	Secure user name and password In secure Exams Office	6 Years
Attendance registers copies		Candidate name Candidate Number	Secure Storage	In secure Exams Office	After Post Results Services
Candidates' scripts		Candidate Legal Name Candidate Number	Secure Storage	Packaged in Exam Room – Stored in Secure Exams Office until collected	That day – next day at latest depending on Parcel Force collection time
Candidates' work		Candidate Legal Name Candidate Number	Teaching classrooms	Secure cupboards	End of academic year – Those kept for teaching and

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
					learning will have the candidate name and any personal information removed
Centre consortium arrangements for centre assessed work	N/A				
Certificates		Candidate Legal Name	Secure Storage	Within stecure exams office – only 4 staff members have access to the storage	1 year
Certificate destruction information		Candidate name Candidate number	Centre secure network	Secure username and password	indefinite
Certificate issue information					
Conflicts of Interest records					
Entry information		Candidate name & Legal name Candidate number	MIS Hard copy in file in exams office	Secure exams office while live and secure storage after 1st year	6 years
Exam room incident logs		Candidate name Candidate number	Paper format in exams office	Secure exams office	After Post Results Services
Invigilator and facilitator training records		Invigilator name	Centre secure network & Hard copy in Policies	Secure exams office	1 year

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
			file for the inspection visit		
Overnight supervision information	This has not yer been relevant				
Post-results services: confirmation of candidate consent information		Candidate name	Hard copy in exams office	Secure exams office	After Post Results Services
Post-results services: requests/outcome information		Candidate name Candidate number	Hard copy in exams office / secure netwrok	Secure exams office / username and password	After Post Results Services
Post-results services: scripts provided by ATS service		Candidate name Candidate number	Given to Head of Department and placed in their secure storage	Candidate information is removed	End of PRS or longer of used for teaching and learning
Post-results services: tracking logs		Candidate name Candidate number	A spreadsheet is created and stored on the centre secure network	Username and password	After Post Results Services
Private candidate information	We do not accept Private Candidates				
Resolving timetable clashes information		Candidate name Candidate number	MIS, Centre secure network	Username and password	6 Years
Results information		Candidate name Candidate number	MIS, secure Exam Board websites, secure storage	Username and password / only 4 staff have access to the secure storage	6 Years
Seating plans		Candidate name Candidate number	Secure exams office until the day before the exams when an	Only accessible by Exams Officer until the day prior to the	After Post Results Services

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
			enlarged copy is put in a locked display cabinet. A copy is given to invigilators and centre staff to complete registers and set up exam rooms	exam, locked display cabinet is only accessible by exams staff. All copies are returned to the exams officer after each exams – completed registers are held in secure storage	
Special consideration information		Candidate name Candidate number Candidate medical information	File in exams office	Secure office in an secure area	6 Years
Suspected malpractice reports/outcomes		Candiate name Candidate number	File in exams office	Secure office in a secure area	10 Years
~~Transfer of credit information~~					
Transferred candidate arrangements	Transferred candidate arrangements	Candidate name Candidate number	MIS if our candidate, Centre secure network if candidate belongs to another Centre. Paperwork in exams office	Secure office in a secure area	6 Years
Very late arrival reports/outcomes	Very late arrival reports/outcomes	Candidate name Candidate number	Exams office, centre secure network, relevant secure Exam Board website	Secure office in a secure area, username and password	6 Years