General Data Protection Regulation Policy (exams)

2024

College Governance Status

This policy is reviewed annually to ensure compliance with current regulations.

Review dates	By Whom	Approval date
February 2020	Staff and Governors	February 2020
March 2022	Staff and Governors	March 2022
March 2023	Staff and Governors	March 2023
January 2024	Staff and Governors	March 2024

Signed by the Chair:

Key staff involved in the policy

Role	Name(s)
Head of centre	**Susan Boyd**
Exams officer & Data Manager	**Michael Okroy**
Exams officer line manager (Senior leader)	**Andrew Whelan**
IT manager	**Tom Hutchinson**

Purpose of the policy

This policy details how Caedmon College Whitby, 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
- Department for Education; Local Authority; 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 Cloudschool 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

Caedmon College Whitby ensures that candidates are fully aware of the information and data held.

All candidates are:

- informed via centre newsletter, electronic and paper communication, etc.
- given access to this policy via centre website, written request, etc.

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 5 – 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**

The 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 6 – 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 7 – 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.

Section 8 – Access to information

Current and former candidates can request access to the information/data held on them by making a **subject access request** to the Exams Officer and/or Data Manager in writing/email and ID will need to be confirmed if a former candidate is unknown to current staff.

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. 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

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)	**All information given to SEN dept once the student has left CCW**
Alternative site arrangements		Candidate name Candidate No.	MIS	Secure Exams Only Area	Destroyed once RoR deadline has passed & during next academic year
Attendance registers copies		Candidate name Candidate No.	Filing Cabinet	In secure Exams office	Destroyed once RoR deadline has passed
Candidates' scripts		Candidate name Candidate No.	Lockable Filing Cabinet until Parcelforce collects	In secure Exams office	NA
Candidates' work		By Teaching Departments			
Centre consortium arrangements for centre assessed work		By Teaching Departments			

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		Candidate name Candidate No. Candidate DOB	Filing Cabinet	In secure Exams office	5 years
Certificate issue information		Candidate name	Archfile	In secure Exams office	ongoing
Conflicts of Interest records		Candidate name Candidate DOB	**MIS**	Secure Exams Only Area	Destroyed once RoR deadline has passed & during next academic year
Entry information		Candidate name	Filing Cabinet MIS	In secure Exams office	Destroyed once RoR deadline has passed & during next academic year
Exam room incident logs		Candidate name	Filing Cabinet	In secure Exams office	Destroyed once RoR deadline has passed & during next academic year
Invigilator and facilitator training records		Invigilator name	Archfile	In secure Exams office	ongoing
Overnight supervision information		Candidate name	Filing Cabinet	In secure Exams office	Destroyed once RoR deadline has passed & during next academic 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
Post-results services: confirmation of candidate consent information		Candidate name Candidate No	Filing Cabinet	In secure Exams office	Retained for 12 months
Post-results services: requests/outcome information		Candidate name Candidate No	Filing Cabinet MIS	In secure Exams office	Retained for 12 months Destroyed once
Post-results services: scripts provided by ATS service		Candidate name Candidate No	MIS	Secure Exams Only Area	Destroyed once RoR deadline has passed & during next academic year
Post-results services: tracking logs		Candidate name Candidate No	MIS	Secure Exams Only Area	Retained for 12 months
Private candidate information		Candidate name Candidate No DOB Address Contact information	Filing Cabinet	In secure Exams office	Retained for 12 months
Resolving timetable clashes information		Candidate name Candidate No	Filing Cabinet	In secure Exams office	Retained for 12 months
Results information		Candidate name Candidate No	Filing Cabinet MIS	In secure Exams office	Current year + 6 previous years
Seating plans		Candidate name Candidate No	Filing Cabinet	In secure Exams office	Destroyed once RoR deadline has passed &

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
					during next academic year
Special consideration information		Candidate name Candidate No	Filing Cabinet	In secure Exams office	Retained for 12 months
Suspected malpractice reports/outcomes		Candidate name Candidate No	Filing Cabinet	In secure Exams office	Recommended Guideline followed
Transferred candidate arrangements		Candidate name Candidate No	Filing Cabinet	In secure Exams office	Destroyed once RoR deadline has passed & during next academic year
Very late arrival reports/outcomes		Candidate name Candidate No	Filing Cabinet	In secure Exams office	Destroyed once RoR deadline has passed & during next academic year