



Data Protection Policy (Exams)

2021/22

This policy is reviewed annually to ensure compliance with current regulations

Approved/reviewed by	
Kevin Bawn	
Date of next review	January 2023

Key staff involved in the policy

Role	Name(s)
Head of centre	Kevin Bawn
Exams officer	Rebecca Dominy
IT manager	Graeme Lee
Data manager	Allen Bailey

Purpose of the policy

This policy details how Clyst Vale Community College, 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 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 (JCQ)

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

- hard copy
- email
- secure extranet sites – eg eAQA; OCR Interchange; Pearson Edexcel Online; WJEC Secure Website.
- our Management Information System (MIS) provided by Capita SIMS for 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

Clyst Vale Community College ensures that candidates are fully aware of the information and data held.

All candidates are:

- informed via our centre newsletter and school assemblies

- given access to this policy via our website.

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 via the Exams Booklet.

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
Desktop computers and laptops which can connect to the secure college network	IT Dept maintain the hardware and update the antivirus software on an ongoing basis.

Software/online system	Protection measure(s)
SIMS Awarding Body secure extranet	Protected usernames & passwords, regular re-setting of passwords, EO creates all new users for AO secures sites and deletes obsolete accounts. IT Dept perform regular checks of Firewall and Antivirus software.

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

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 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.

The table below details the type of candidate exams-related information held, and how it is managed, stored and protected

Protection measures include:

- password protected area on the centre's intranet
- secure drive accessible only to selected staff
- information held in secure area
- updates undertaken every regularly by IT Dept

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 Exams Officer.

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 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.

Requesting exam information

Requests for exam information can be made to the Exams Officer or the Data Protection Officer in writing or via email. If a former candidate requests information they will need to provide photographic ID before any information is released.

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, is provided.

In the case of looked-after children or those in care, agreements are already 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 legislation and guidance regarding sharing information with parents (including non-resident parents), for 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

Clyst Vale Community College will publish exam results to the media or within the centre 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.

As Clyst Vale Community College 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 the Exams Officer (as outlined in the college handbooks).

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	What personal/sensitive data is/may be contained in the information	Where information is stored	How information is protected
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 Within Additional Support office	Secure user name and password Secure user name and password In secure office
Attendance registers copies	Candidate names & numbers with exam entry information	Securely in the Exams Office	Secure key card needed to get into Exams Office
Certificates	Candidates names and results	Securely in the Exams Office	Secure key card needed to get into Exams Office
Certificate issue information	Candidates names	Securely in the Exams Office	Secure key card needed to get into Exams Office
Conflicts of Interest records	Staff names & nature of conflict	Securely in the Exams Office	Secure key card needed to get into Exams Office
Exam room incident logs, seating plans, registers etc	Candidate information during exams	Securely in the Exams Office	Secure key card needed to get into Exams Office
Invigilator and facilitator training records	Names & completion dates	Securely in the Exams Office	Secure key card needed to get into Exams Office
Post-results services documentation	Candidates names & exams they wish to appeal	Securely in the Exams Office	Secure key card needed to get into Exams Office

Information type	What personal/sensitive data is/may be contained in the information	Where information is stored	How information is protected
Results information	Candidates names & exam results	Securely in the Exams Office	Secure key card needed to get into Exams Office
Special consideration information	Candidates names & details of problems affecting their exams	Securely in the Exams Office	Secure key card needed to get into Exams Office
Suspected malpractice reports/outcomes	Candidates names & details of suspected malpractice and outcomes	Securely in the Exams Office	Secure key card needed to get into Exams Office