



PLUME

Maldon's Community Academy

DATA PROTECTION POLICY

(Exams)

2022/23

This policy is reviewed annually to ensure compliance with current regulations

Approved/reviewed by	
Mrs R Clark	
Date of next review	December 2023

Key staff involved in the policy

Role	Name(s)
Head of centre	Carl Wakefield
Exams officer	Beverley Chittock
Senior leader(s)	Ruth Clark/Tom Baster
IT manager	Mark Beckett
Data manager	Richard Scott

Contents

Key staff involved in the policy	2
Purpose of the policy	4
Section 1 – Examinations-related information	4
Section 2 – Informing candidates of the information held	5
Section 3 – Hardware and software	5
Section 4 – Dealing with data breaches	5
Section 5 – Candidate information, audit and protection measures.....	6
Section 6 – Data retention periods	7
Section 7 – Access to information.....	7
Section 8 – Table recording candidate exams-related information held	9

Purpose of the policy

This policy details how Plume Academy, in relation to examinations 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 JCQ's [General Regulations for Approved Centres](#) (section 6.1) 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.

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 examinations 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' examination information – even that which is not classified as personal or sensitive – is covered under this policy.

Section 1 – Examinations-related information

There is a requirement for the examinations office to hold examinations-related information on candidates taking external examinations. For further details on the type of information held please refer to Section 5 below.

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

- Awarding bodies
- Joint Council for Qualifications (JCQ)
- Department for Education; Local Authority; the Press; other schools

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

- hard copy
- email
- examination boards' secure extranet site(s) – AQA Centre Services; OCR Interchange; Pearson Edexcel Online; WJEC Secure Website
- MIS provider (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.
- DfE Connect
- Schools to Schools

This data may relate to examination entries, access arrangements, the conduct of examinations and non-examination assessments, special consideration requests and examination results/post-results/certificate information.

Section 2 – Informing candidates of the information held

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

All candidates are:

- informed via their examination statement of entry
- given access to this policy via the Plume Academy website

Candidates are made aware of the above when the entries are submitted to awarding bodies for processing.

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 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 using *Access arrangements online* are also required to provide their consent by signing the GDPR compliant JCQ candidate personal data consent form before 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	Warranty expiry
Desktop computer; Laptop	Checks: Firewall correctly configured Hardware protected by Encryption key Scheduled virus check	N/A

Software/online system	Protection measure(s)
DfE Connect School to School	Protected usernames and passwords
MIS, SIMS, A2C	Protected usernames and passwords Regular checks to Firewall/Antivirus software
Awarding body secure extranet sites	Centre administrator (EO) has to approve the creation of new user accounts and determine access rights Protected usernames and passwords

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 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' examination-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 examinations-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 automatically and as necessary (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 from the Examinations Officer.

Section 7 – Access to information

(With reference to ICO information <https://ico.org.uk/your-data-matters/schools/exam-results/>)

The GDPR gives individuals the right to see information held about them. This means individuals can request information about them and their examination 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 examination questions.

Requesting examination information

Requests for examination information can be made to the Examinations Officer via exams@plume.essex.sch.uk. If a former candidate is unknown to current staff, an extra form of ID will be required, e.g. date of birth.

The GDPR does not specify an age when a child can request their examination 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 the 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 examination information before examination 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 examination 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.

Unless otherwise defined within this policy, candidates' personal data will not be shared with a third party.

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

Candidate data information will not be shared with parents without the candidate's explicit consent.

Publishing examination results

When considering publishing examination results, Plume Academy will make reference to the ICO (Information Commissioner's Office) <https://ico.org.uk/your-data-matters/schools/exam-results/> Can schools give my exam results to the media for publication?

Plume Academy will publish examination 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

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	Minimum Retention period
Access arrangements information		Candidate name, 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 Secure user name and password In secure office (SENCo)	Until candidate's final exam series
Alternative site arrangements	Hard copies of CAP submission	May show candidate home address	Lockable metal filing cabinet	In secure office	Until deadline for review of marking has passed
Attendance registers copies	Hard copies	Candidate name and number	Lockable metal filing cabinet	In secure office	Until deadline for review of marking has passed
Candidates' scripts	Unwanted copies of scripts returned to centre via ATS	Candidate name, number and sometimes signature	Lockable metal filing cabinet	In secure office	Until deadline for review of marking has passed
Candidates' work	NEA work returned to centre by awarding body at end of moderation period	Candidate name, number, DOB, signature	MIS Lockable metal filing cabinet	Secure user name & password In secure office or faculty office	Until deadline for review of marking 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	Minimum Retention period
Certificates		Candidate name, number, DOB	Filing cabinet	Secure office	Until certificates issued to candidates Any unclaimed for at least 12 months
Certificate destruction information		Candidate name, number	Filing cabinet	Secure office	Four years
Certificate issue information		Candidate name, DOB, number	Filing cabinet	Secure office	Seven years
Conflicts of interest records		Staff name, job title, signature Candidate name, number, relationship to staff member	Lockable metal filing cabinet	Secure office	Until deadline for review of marking has passed
Entry information		Candidate name, number, DOB, access arrangement, UCI, ULN	MIS	Secure user name & password	Archived after deadline for review of marking has passed
Exam room incident logs		Candidate name	Lockable metal filing cabinet	Secure office	Until deadline for review of marking has passed
Invigilator and facilitator training records		Invigilator name, signature	Lockable metal filing cabinet R drive/Exams	Secure office Secure user name & password	Updated annually
Overnight supervision information	Hard copy of CAP form Declaration form	Candidate name, number Candidate name, signature and Supervisor name, signature	Lockable metal filing cabinet	Secure room	Until deadline for review of marking has passed
Post-results services: confirmation of candidate consent information		Candidate name, number, signature	Lockable metal filing cabinet	Secure room	Until 6 months after review of result outcome

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	Minimum Retention period
Post-results services: requests/outcome information		Candidate name, number	Lockable metal filing cabinet R drive/Exams	Secure room Secure user name & password	Until 6 months after review of result outcome
Post-results services: scripts provided by ATS service		Candidate name, number and possibly signature	Lockable metal filing cabinet until forwarded to candidate/teacher	Secure room	Forwarded to candidate/teacher
Post-results services: tracking logs		Candidate name, number	MIS	Secure user name & password	Until 6 months after review of result outcome
Private candidate information		Candidate name, number, email, postal address, DOB	Lockable metal filing cabinet	Secure room	Until deadline for review of marking has passed
Results information		Candidate name, number, grades	MIS Lockable metal filing cabinet	Secure user name & password Secure room	At least 6 years
Seating plans		Candidate name, number, access arrangements	MIS Lockable metal filing cabinet	Secure user name & password Secure room	Until deadline for review of marking has passed
Special consideration information	Hard copy of application to awarding body & evidence	Candidate name, number, DOB, details/evidence	Lockable metal filing cabinet	Secure room	Until deadline for review of marking has passed
Suspected malpractice reports/outcomes	Hard copy of report to awarding body	Candidate name, number, details/evidence	Lockable metal filing cabinet	Secure room	Until deadline for review of marking 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	Minimum Retention period
Transferred candidate arrangements	Hard copy of application submitted via JCQ CAP	Candidate name, number, details	Lockable metal filing cabinet	Secure room	Until deadline for review of marking has passed
Very late arrival reports/outcomes	Hard copy of application submitted via JCQ CAP	Candidate name, number, details	Lockable metal filing cabinet	Secure room	Until deadline for review of marking has passed