

# **Data Protection Policy 2024/25**

The Basildon Upper Academy

## Data Protection Policy 2024/25

Centre Name	The Basildon Upper Academy
Centre Number	16133
Date policy first created	16/09/2024
Current policy approved by	Rebecca Rees
Current policy reviewed by	Sophie Rowe
Date of next review	30/09/2024

## Key staff involved in the policy

Role	Name
Head of centre	Rebecca Rees
Senior leader(s)	Sharon Szuszkiewicz
Exams officer	Sophie Rowe
IT Manager	Jeff Archer
Data Manager	Philip Beaumont
Other staff (if applicable)	

## **Purpose of the policy**

This policy details how The Basildon Upper 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 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.

It is the responsibility of the centre to inform candidates of the processing that the centre undertakes. For example, that the centre will provide relevant personal data including name, date of birth, gender to the awarding bodies for the purpose of examining and awarding qualifications.

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

To ensure that the centre meets the requirements of the DPA 2018 and UK 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 below.

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 site(s) – AQA Centre Services; OCR Interchange; Pearson Edexcel Online; WJEC Portal
- Bromcom

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

## **Section 2 – Informing candidates of the information held**

The Basildon Upper Academy ensures that candidates are fully aware of the information and data held.

All candidates are:

- informed via centre newsletter and text message.

- given access to this policy via centre website.

Candidates are made aware of the above at the start of a course or when the registrations/entries are submitted to awarding bodies for processing.

Materials which are submitted by candidates for assessment may include any form of written work, audio and visual materials, computer programmes and data (“Student Materials”). Candidates will be directed to the relevant awarding body’s privacy notice if they require further information about how their Student Materials may be used by the awarding body.

Candidates eligible for access arrangements/reasonable adjustments 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	Date of purchase and protection measures	Warranty expiry
Computer	The IT team annually check the hardware systems in the school to ensure everything is in working order.	N/A

Software/online system	Protection measure(s)
Bromcom	All members of staff have access to bromcom, but certain staff have certain access. All staff have their own unique password and username.

### 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 headteacher and CEO 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 every 6-12 months.

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 every 6 months (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 from the exams officer in the data office.

## **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 exam 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 exam questions.

### **Requesting exam information**

Requests for exam information can be made to the exams officer via email/ phone or in person.

The GDPR does not specify an age when a child can request their exam 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.

### **Responding to requests**

If a request is made for exam information before exam 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 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.

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 and a local authority (the 'corporate parent'), 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](http://www.gov.uk/government/publications/dealing-with-issues-relating-to-parental-responsibility/understanding-and-dealing-with-issues-relating-to-parental-responsibility)  
(Updated 24 August 2023 to include guidance on the role of the 'corporate parent', releasing GCSE results to a parent and notifying separated parents about a child moving school)
- School reports on pupil performance  
[www.gov.uk/guidance/school-reports-on-pupil-performance-guide-for-headteachers](http://www.gov.uk/guidance/school-reports-on-pupil-performance-guide-for-headteachers)

### **Publishing exam results**

When considering publishing exam results, The Basildon Upper 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?

OR

The Basildon Upper Academy 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 The Basildon Upper Academy will have a legitimate reason for publishing examination results, consent is not required from students or their parents/carers for publication. However, if a student or their parents/carers 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, 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.