**THE KING DAVID HIGH SCHOOL**

# Data Protection (Exams) Policy

2026-2027

This policy is reviewed annually to ensure compliance with current regulations

| Approved/reviewed by | |
|---|---|
| Tracy Basger | |
| Date of next review | 31 October 2027 |

## Key staff involved in the policy

| Role | Name(s) |
|---|---|
| Head of centre | **Tracy Basger** |
| Exams officer | **Joanna Hipkiss** |
| Senior leader(s) | **Tim Chappelle, Jack Pitt, Paula Watson, Jocelyn Buckley-Dibben** |
| IT manager | **Harvey Marks** |
| Data manager | **Joanna Hipkiss** |

## Contents

**Key staff involved in the policy** Error! Bookmark not defined.

**Purpose of the policy** Error! Bookmark not defined.

**Section 1 – Exams-related information** Error! Bookmark not defined.

**Section 2 – Informing candidates of the information held** Error! Bookmark not defined.

**Section 3 – Hardware and software** Error! Bookmark not defined.

**Section 4 – Dealing with data breaches** Error! Bookmark not defined.

**Section 5 – Candidate information, audit and protection measures** Error! Bookmark not defined.

**Section 6 – Data retention periods** Error! Bookmark not defined.

**Section 7 – Access to information** Error! Bookmark not defined.

**Section 8 – Table recording candidate exams-related information held** Error! Bookmark not defined.

## Purpose of the policy

This policy details how The King David High School 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)
- Department for Education

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 Secure Website;
- SIMS/ sending/receiving information via electronic data interchange (EDI) using A2C to/from awarding body

This data may relate to exam entries, access arrangements, including controlled assessments and coursework, 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

The King David High School ensures that candidates are fully aware of the information and data held.

All candidates are:

- informed via email
- given access to this policy via the school website

Candidates and parents/carers are provided with access to the school's privacy notice when personal data is collected, or within the timescales required by UK GDPR. The notice explains how examination-related personal data is used, shared, stored and retained, including sharing with awarding bodies.

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 requiring access arrangements or reasonable adjustments will be informed that their personal data will be processed using Access Arrangements Online in accordance with UK GDPR and the Data Protection Act 2018. The SENCo will retain the required evidence and records in accordance with JCQ regulations.

## 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 |
|---|---|---|
| Desktops<br>Laptops | IT Department update antivirus software | Contact IT Dept for individual warranty information |

| Software/online system | Protection measure(s) |
|---|---|
| MIS-SIMS<br>Awarding Body extranet sites | Usernames and password protected<br>Passwords changed regularly |

## 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**

Data Protection Officer and Head of Centre 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.

All suspected personal data breaches must be reported immediately to the school's Data Protection Officer (DPO).

The DPO will assess whether the breach must be reported to the Information Commissioner's Office (ICO). Where notification is required, the ICO will be informed without undue delay and, where feasible, within 72 hours of the school becoming aware of the breach.

Where a breach is likely to result in a high risk to individuals' rights and freedoms, affected individuals will also be informed without undue delay, unless a legal exception applies.

All personal data breaches, including those not requiring notification to the ICO, will be documented in the school's data breach register.

**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 may include:

- password protected area on the centre's intranet
- secure drive accessible only to selected staff
- information held in secure area
- security updates, antivirus protection and software patches are managed by the IT department and applied promptly in accordance with the school's Cyber Security Policy

Examination-related records will be retained only for as long as necessary for its specified purposes and securely disposed of in accordance with the school's approved Data Protection policy, taking account of JCQ and awarding body requirements and applicable data protection legislation.

## 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 access to personal information may be made verbally or in writing and will be referred promptly to the school's Data Protection Officer. Requests will be handled in accordance with UK GDPR and applicable statutory timescales, including the specific provisions relating to examination information.

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.

A decision will be made by the 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 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 only be shared with authorised third parties where there is a lawful basis for doing so, in accordance with UK GDPR, the Data Protection Act 2018 and the school's privacy notice.

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 '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
- School reports on pupil performance
  www.gov.uk/guidance/school-reports-on-pupil-performance-guide-for-headteachers

**Publishing exam results**

Where the school publishes candidates' examination results, it will do so in accordance with UK GDPR, the Data Protection Act 2018 and Information Commissioner's Office guidance.

Candidates and parents/carers will be informed in advance where and how results may be published.

The school will ensure that publication has an appropriate lawful basis and will consider any objections raised by candidates or parents/carers before publication. Any objections will be referred to the Data Protection Officer for consideration.

## 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 | Retention period |
|---|---|---|---|---|
| Access arrangements information | Candidate name<br>Candidate DOB<br>Gender<br>Diagnostic testing outcome(s)<br>Specialist report(s) (may also include candidate address)<br>Evidence of normal way of working | Access Arrangements Online<br>MIS<br>Lockable metal filing cabinet | Secure user name and password and MFA<br>In secure office (SENCo) | 7 years |
| Alternative site arrangements | NA | | | |
| Attendance registers copies | Candidate name<br>Candidate DOB<br>Gender | Exams Office | Secure room | Retained until the deadline for reviews of marking has passed, or until any appeal, malpractice investigation or other results enquiry has been completed, whichever is later. |
| Candidates' scripts | Candidate name | Exam boards' online script-viewer functions<br>Microsoft Outlook | Secure user name and password and MFA | To end of academic year |
| Candidates' work | Candidate name | Exam boards' online platform | Secure user name and password and MFA | Refer to exam board's data retention policy |

| Information type | What personal/sensitive data is/may be contained in the information | Where information is stored | How information is protected | Retention period |
|---|---|---|---|---|
| | | | | |
| Certificates | Candidate name<br>Candidate DOB | Locked secure storage | Secure room | 7 years |
| Certificate destruction information | Candidate name<br>Candidate DOB<br>Results | Secure space on computer | Secure user name and password and MFA | 4 years from the date of destruction, in accordance with JCQ General Regulations. |
| Certificate issue information | Candidate name<br>Candidate DOB<br>Results | Exam boards' online platform<br>**MIS** | Secure user name and password and MFA | **7 years** |
| Conflicts of interest records | Candidate name<br>Candidate family links | Secure space on computer | Secure user name and password and MFA | 7 years |
| Entry information | Candidate name<br>Candidate DOB | MIS | Secure user name and password and MFA | 7 years |
| Exam room incident logs | Candidate name/Exam no | Exams Office | Secure room | Retained until the deadline for reviews of marking has passed, or until any appeal, malpractice investigation or other results enquiry has been completed, whichever is later. |
| Invigilator and facilitator training records | Staff name<br>Training records | Exams Office | Secure room | Retained until the deadline for reviews of marking has |

| Information type | What personal/sensitive data is/may be contained in the information | Where information is stored | How information is protected | Retention period |
|---|---|---|---|---|
| | | | | passed, or until any appeal, malpractice investigation or other results enquiry has been completed, whichever is later. |
| Overnight supervision information | Candidate name/Exam no | Exams Office | Secure room | Retained until the deadline for reviews of marking has passed, or until any appeal, malpractice investigation or other results enquiry has been completed, whichever is later. |
| Post-results services: confirmation of candidate consent information | Candidate name/Exam no | Microsoft programme on computer | Secure user name and password and MFA | Retained until the deadline for reviews of marking has passed, or until any appeal, malpractice investigation or other results enquiry has been completed, whichever is later. |
| Post-results services: requests/outcome information | Candidate name/Exam no<br>Results | Microsoft programme on computer | Secure user name and password and MFA | Retained until the deadline for reviews of marking has passed, or until any appeal, malpractice investigation or other results enquiry has been completed, whichever is later. |

| Information type | What personal/sensitive data is/may be contained in the information | Where information is stored | How information is protected | Retention period |
|---|---|---|---|---|
| Post-results services: scripts provided by ATS service | Candidate name | Exam boards' online script-viewer functions<br>Microsoft Outlook | Secure user name and password and MFA | To end of academic year |
| Post-results services: tracking logs | Candidate name/Exam no | Microsoft programme on computer | Secure user name and password and MFA | Retained until the deadline for reviews of marking has passed, or until any appeal, malpractice investigation or other results enquiry has been completed, whichever is later. |
| Resilience arrangements: Evidence of candidate performance | Candidate name | In Departments. On MIS | Secure user name and password and MFA | Department-led |
| Resolving timetable clashes information | NA | | | |
| Results information | Candidate name/Exam no<br>Results | Exams Office<br>On MIS<br>SISRA & FFT | Locked office<br>Secure user name and password and MFA | 7 years in office<br>SISRA – until the pupil reaches the age of 25<br>FFT – 5 years |
| Seating plans | Candidate name/Exam no<br>Access arrangements | Exams Office – MIS computer | Locked office<br>Secure user name and password and MFA | 7 years |
| Special consideration information | Candidate name/ Exam No<br>Personal circumstances | Exams Office- computer | Locked office<br>Secure user name and password and MFA | Retained until the deadline for reviews of marking has passed, or until any appeal, malpractice investigation or other |

| Information type | What personal/sensitive data is/may be contained in the information | Where information is stored | How information is protected | Retention period |
|---|---|---|---|---|
| | | | | results enquiry has been completed, whichever is later. |
| Suspected malpractice reports/outcomes | Candidate name/ Exam No | Exams Office- computer | Locked office<br>Secure user name and password and MFA | Retained until the deadline for reviews of marking has passed, or until any appeal, malpractice investigation or other results enquiry has been completed, whichever is later. |
| Transferred candidate arrangements | NA | | | |
| Very late arrival reports/outcomes | Candidate name/ Exam No | Exams Office- computer | Locked office<br>Secure user name and password and MFA | Retained until the deadline for reviews of marking has passed, or until any appeal, malpractice investigation or other results enquiry has been completed, whichever is later. |