

**DATA PROTECTION POLICY (Exams)**

2024/25

This policy is reviewed annually to ensure compliance with current regulations

|  |  |
| --- | --- |
| Approved/reviewed by | |
| Rachel Baroni | |
| Date of next review | 30/09/2025 |

Key staff involved in the policy

|  |  |
| --- | --- |
| Role | Name(s) |
| Head of centre | Russell Harris |
| Exams officer | Michelle Hutchinson |
| Senior leader(s) | Gary Hennigan, Andy Rosie, Rachel Baroni, Kasia Davies |
| IT manager | Andy Church |
| Data manager | Emma Oosthuizen, Kingsley Sawyers |

Contents

[Key staff involved in the policy 2](#_Toc175686045)

[Purpose of the policy 4](#_Toc175686046)

[Section 1 – Exams-related information 4](#_Toc175686047)

[Section 2 – Informing candidates of the information held 5](#_Toc175686048)

[Section 3 – Hardware and software 5](#_Toc175686049)

[Section 4 – Dealing with data breaches 6](#_Toc175686050)

[Section 5 – Candidate information, audit and protection measures 7](#_Toc175686051)

[Section 6 – Data retention periods 7](#_Toc175686052)

[Section 7 – Access to information 7](#_Toc175686053)

[Section 8 – Table recording candidate exams-related information held 10](#_Toc175686054)

Purpose of the policy

This policy details how Fulford 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](https://www.jcq.org.uk/exams-office/general-regulations/) (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
* Local Authority
* The wider Multi Academy Trust
* Press releases

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
* MIS system – ESS SIMS
* Sending and receiving information through the electronic data interchange (EDI) using A2C

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

Fulford School ensures that candidates are fully aware of the information and data held.

All candidates are:

* informed via electronic and verbal communication, e.g., assemblies, class charts, letters home.
* given access to this policy via the exams section of the school website.

Candidates are made aware of the above at the start of a course and when 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 |
| Exam Officer’s Desktop | Purchased: Jan 2020.   * Checked monthly by IT team * Antivirus software installed and updated * Hard drives securely wiped and destroyed upon decommissioning | N/A |
| Exam Assistant’s Desktop | Purchased: Jan 2020.   * Checked monthly by IT team * Antivirus software installed and updated * Hard drives securely wiped and destroyed upon decommissioning | N/A |
| Exam Office Desktop | Purchased: Mar 2016.   * Checked every term by IT team * Located in a locked room which only authorised personnel has access to * Antivirus software installed and updated * Hard drives securely wiped and destroyed upon decommissioning | N/A |
| Server (Data Storage) | * Regular backups performed * Access restricted to authorised personnel only | N/A |

|  |  |
| --- | --- |
| Software/online system | Protection measure(s) |
| Management Information System (MIS) | * Accounts can only be created by authorised personnel * Role-based access controls * Only accessible from specific devices |
| Internet Browsers (Chrome, Edge) | * Web and firewall filtering enabled via Smoothwall * Suspicious sites blocked * Automatic updates applied * Application is locked down via IT policies |

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 IT Manager 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

1. **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?

1. **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.

1. **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 annually.

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 regularly and as required (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 Exams Manager.

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 main school office in writing and this will be passed on to the Data Protection Officer. ID may be required. This follows the schools Subject Access Request process.

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 Data Protection Officer 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 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 (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](https://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, Fulford School 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?  As Fulford School 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 main school office and then passed to the Data Protection 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. |

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  Signed candidate personal data consent form  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 username and password only accessible by SENCo, assessor and Exams Manager  In secure office (exams) | Until candidates 25th birthday when purged from the system or securely destroyed |
| Alternative site arrangements |  | Candidate name  Candidate number  Candidate DOB | Access Arrangements Online | Secure username and password only accessible by SENCo, assessor and Exams Manager | 12 months |
| Attendance registers copies |  | Candidate name  Candidate number | In the exam secure office room | Room is locked, only exams staff have keys | 12 months |
| Candidates’ scripts |  | Candidate name  Candidate number | Send to awarding bodies immediately following completion of the exam (same day or next day)  Kept in a locked safe in the exams secure office until collected by Parcel Force | Room is locked, only exams staff have keys | 24 hours maximum |
| Candidates’ work |  | Candidate name  Candidate number | Sent to awarding bodies if requested as part of a sample  Subject departments keep all others secure | Subject department lockable storage | Until after the deadline for post results requests and appeals has past, or for at least 6 months |
| Centre consortium arrangements for centre assessed work |  | n/a | n/a | n/a | n/a |
| Certificates |  | Candidate name  Candidate DOB  Candidate number  Candidate UCI and ULN numbers  Qualification grades | Lockable metal filing cabinet (reception) | Restricted staff access to the keys | 5 years |
| Certificate destruction information |  | Candidate name  Candidate number  Qualification grades | On exams drive | Password protected file | 4 years after destruction |
| Certificate issue information |  | Candidate name | Lockable metal filing cabinet (reception) | Restricted staff access to the keys | 5 years |
| Conflicts of interest records |  | Candidate name | On exams drive | Only accessible with username and password | 12 months |
| Entry information |  | Candidate name  Candidate number | MIS  Awarding body secure sites | Only accessible with username and password | 18 months |
| Exam room incident logs |  | Candidate name  Candidate number | In the exam secure office room | Room is locked, only exams staff have keys | 12 months |
| Invigilator and facilitator training records |  | Invigilator name | TEO Hub  Training record folder | Only accessible with username and password  Exam secure office – only exams staff have keys | 18 months |
| Overnight supervision information |  | Candidate name  Candidate number | In the exam secure office room | Room is locked, only exams staff have keys | 12 months |
| Post-results services: confirmation of candidate consent information |  | Candidate name  Candidate number | On exams drive  Paper forms in a locked metal filing cabinet | Only accessible with username and password  Only exams staff have keys | 12 months |
| Post-results services: requests/outcome information |  | Candidate name  Candidate number | On exams drive | Only accessible with username and password | 12 months |
| Post-results services: scripts provided by ATS service |  | Candidate name  Candidate number | On the exams team drive and with the relevant teachers to be used as examples | Only accessible by exams staff and relevant teachers.  Personal information redacted before using as example. | Redacted – as long as the work is still relevant to the subject qualification framework |
| Post-results services: tracking logs |  | Candidate name  Candidate number | On exams drive | Only accessible with username and password | 12 months |
| Private candidate information |  | Candidate name  Candidate number  Candidate UCI and ULN numbers  Address, email and telephone number | MIS  Paper forms in a locked metal filing cabinet | Only accessible with username and password  Only exams staff have keys | 12 months |
| Resilience arrangements: Evidence of candidate performance | Candidate mock exam papers sat under exam conditions | Candidate name  Candidate number | Secure exams drive | Only accessible by username and password | 12 months |
| Resolving timetable clashes information |  | Candidate name  Candidate number | Secure exams drive | Only accessible by username and password | 12 months |
| Results information |  | Candidate name  Candidate number  Qualification grades | Secure exams drive  MIS  Awarding body secure sites  SLT results folders | Only accessible by username and password  SLT to keep securely locked away | Until candidates 25th birthday when purged from the system |
| Seating plans |  | Candidate name  Candidate number | In the exam secure office room | Room is locked, only exams staff have keys | 12 months |
| Special consideration information |  | Candidate name  Candidate number  Reason for special consideration including any medical evidence | Secure exams drive  Awarding body secure sites | Only accessible by username and password | 12 months |
| Suspected malpractice reports/outcomes |  | Candidate name  Candidate number  Reason for malpractice | Secure exams drive | Only accessible by username and password | 12 months |
| Transferred candidate arrangements |  | Candidate name  Candidate number | Secure exams drive | Only accessible by username and password | 12 months |
| Very late arrival reports/outcomes |  | Candidate name  Candidate number | Secure exams drive | Only accessible by username and password | 12 months |