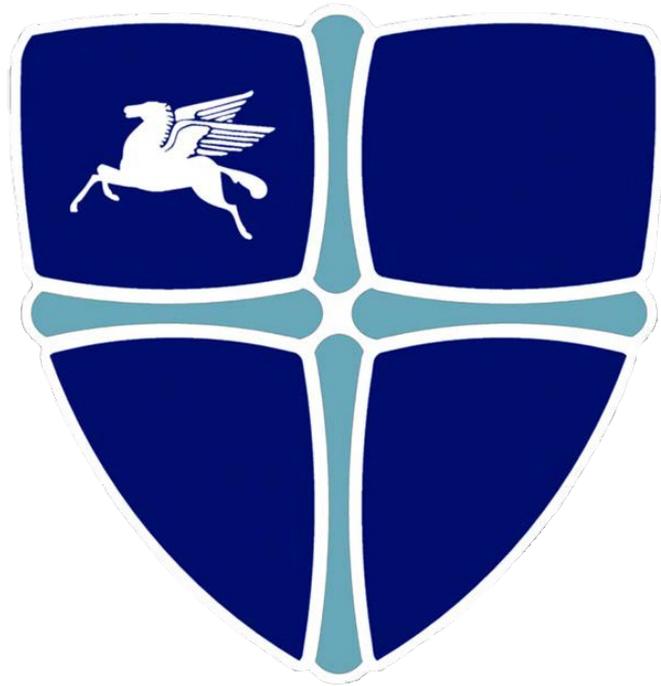


Wellfield School

Data Protection Policy (Exams)



Policy Reviewed: September 2022

Review date: September 2023 (or when new guidance is issued)

Headteacher: Ms. Z. S. Hammond

Exams Manager: Mr. A. E. Pearson

Purpose of the policy

This policy details how Wellfield 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 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 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 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 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 Press

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

- hard copy
- email
- secure extranet site(s) – eAQA; OCR Interchange; Pearson Edexcel Online; WJEC Secure Website, NCFE.
- Management Information System (MIS) provided by Capita SIMS, sending/receiving information via electronic data interchange (EDI) using A2C (<https://www.jcq.org.uk/about-a2c>) to/from awarding body processing systems.

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

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

All candidates are:

- given access to this policy via the school website

Candidates are made aware of the above at the start of their course of study leading to a vocational qualification, or, where candidates are following GCE and GCSE qualification 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 (AAO) are also required to provide their consent by signing the GDPR compliant JCQ candidate personal data consent form 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	Date of purchase and protection measures	Warranty expiry
User Devices Dell Optiplex 3010 Apple iPad (6 th Generation) HP 255 G7	Dell 3010 July 2012, Apple iPad March 2018 and HP 255 G7 November 2019. System updates are centrally managed and deployed regularly. Antivirus software is cloud based and updated automatically. Computer activity is monitored and logged with Impero to ensure compliance.	
Servers Dell PowerEdge R630 Dell MD3420 SAN	Servers and SAN purchased June 2016 Server infrastructure utilises virtualisation (Hyper-V) and is load balanced across multiple servers for resilience. Access to the servers and school infrastructure is limited to the IT Team. Just like the user devices updates and antivirus applications are centrally managed. Servers are regularly backed up to provide resilience in the event of a failure.	

Software/online system	Protection measure(s)
------------------------	-----------------------

SIMS (inc Exams Organiser)	All accounts are password protected and only specified and authorised personnel have access to Exams information.
Internet	Username are randomly generated and difficult to guess. Complex passwords are used and passwords are regularly changed. Internet access is monitored and filtered by Smoothwall access is regularly monitored and access rules are constantly updated to govern Internet access.
A2C	Only installed on one computer in school and only made accessible to the school Exams Officer.
Exam Board Online Secure Sites	Account information and details only available to school Exams Officer. Exams Officer is also the only person able to approve the creation of new accounts to access the secure sites of the exam boards.

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

Mrs. Val Gray will lead on investigating the breach in collaboration with our DPO, Data2Action.

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 biannually at least.

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 checks undertaken weekly and updates applied 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/accessible 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 Mr Pearson, Transport and Exams Manager in writing/email. A Statement of Results or Certificates can only be collected from the school by the person showing Photographic ID which includes date of birth and their full name e.g. Driving License, Passport.

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 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 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.

Publishing exam results

Wellfield School 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 Wellfield 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 [insert name/role of individual], 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 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 In secure office (SENCo)	Retained as long as pupil records are as defined in the schools DP/Retention policy
Alternative site arrangements		Candidate name Candidate DOB Gender	MIS Confirmation notice	Secure username and password In secure office (AEP)	To be kept until the deadline for EARs and the resolution of any outstanding enquiries/appeals
Attendance registers copies		Candidate name Candidate DOB Gender	Lockable metal filing cabinet		Until the deadline for EARs/RoR or the resolution of outstanding appeals/enquiries for relevant exam season.
Candidates' scripts		Candidate name Candidate signature	Secure Storage once exam has ended	In secure storage area. Restricted access (AEP and DR only)	N/A
Candidates' work		Candidate name			Retained until the Pot-results period has

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
		Candidate signature			lapsed for that exams series
Centre consortium arrangements for centre assessed work		N/A			N/A
Certificates		Candidate name Candidate DOB	Lockable filing cabinet	In secure filing cabinet and secure room with restricted access	Retained securely for 10 years from date of issue
Certificate destruction information		Candidate name Date of destruction	Exams Office	Locked Filing cabinet	Retained as long as pupil records are as defined in the schools DP/Retention policy
Certificate issue information		Candidate name		In secure filing cabinet and secure room with restricted access	Retained as long as pupil records are as defined in the schools DP/Retention policy
Conflicts of Interest records		Staff name Name of related person Relationship to staff member Staff signature	Conflict of Interest forms Conflict of Interest Log	In secure office (AEP) Secure user name and password	To be kept until the deadline for EARs and the resolution of any outstanding enquiries/appeals
Entry information		Candidate name Candidate DOB Gender Candidate UCI Candidate ULN	MIS	Secure user name and password	Retained until the Post-results period has lapsed for that exams series
Exam room incident logs		Candidate name	Exam Days file	In secure office (AEP)	Retained until the Post-results period has

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
					lapsed for that exams series
Invigilator and facilitator training records		Invigilator name	Exam Days file	In secure office (AEP)	12 months
Overnight supervision information		Candidate name	Exam Days file	In secure office (AEP)	Retained indefinitely for JCQ inspection purposes
Post-results services: confirmation of candidate consent information		Candidate name Candidate number Candidate signature	PRS request form in lockable filing cabinet	In secure office (AEP)	EAR consent to be retained for at least six months following the outcome of the enquiry or any subsequent appeal. ATS consent to be retained for at least six months from the date consent given.
Post-results services: requests/outcome information		Candidate name Candidate number Candidate result	Lockable filing cabinet	In secure office (AEP)	Six months post outcome/appeal
Post-results services: scripts provided by ATS service		Candidate name Candidate number Candidate signature	Awarding body secure site Where scripts are retained by the centre, they are securely stored (including any electronic versions) and not edited in any way or disposed of until after the awarding body deadline.	Secure user name and password. Restrictions in place as to which staff have access. Access permissions reviewed at least annually	N/A

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
Private candidate information		Candidate name Candidate DOB Gender	MIS Lockable filing cabinet	Secure user name and password. In secure office (AEP)	To be kept until the deadline for EARs and the resolution of any outstanding enquiries/appeals
Resolving timetable clashes information		Candidate name Candidate DOB Gender	MIS Lockable filing cabinet	Secure user name and password. In secure office (AEP)	To be kept until the deadline for EARs and the resolution of any outstanding enquiries/appeals
Results information		Candidate name Candidate DOB Gender Candidate result	MIS Lockable filing cabinet	Secure user name and password. In secure office (AEP)	Records for current year plus 6 previous years to be retained as a minimum
Seating plans		Candidate name Candidate number	MIS Lockable filing cabinet	Secure user name and password. In secure office (AEP)	To be kept until the deadline for EARs and the resolution of any outstanding enquiries/appeals
Special consideration information		Candidate name Candidate DOB Candidate gender Candidate signature Staff name/signature	MIS Lockable filing cabinet	Secure user name and password. In secure office (AEP)	To be kept until the deadline for EARs and the resolution of any outstanding enquiries/appeals
Suspected malpractice reports/outcomes		Staff name	Network area Lockable filing cabinet	Secure user name and password. In secure office (AEP)	To be kept until the deadline for EARs and the resolution of any outstanding enquiries/appeals

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
Transferred candidate arrangements		Candidate name Candidate DOB Candidate gender	MIS Lockable filing cabinet	Secure user name and password. In secure office (AEP)	To be retained until the transfer arrangements are confirmed by the awarding body
Very late arrival reports/outcomes		Candidate name Candidate number Candidate DOB Candidate gender	MIS Lockable filing cabinet	Secure user name and password. In secure office (AEP)	To be kept until the deadline for EARs and the resolution of any outstanding enquiries/appeals for the relevant exams series.