Welland Park Academy

DATA PROTECTION POLICY (EXAMS)

Policy is aligned to current JCQ regulations effective from:	**September 2024**
Agreed with Support Staff Trade Unions	**n/a**
Adopted by the Governing Body	**Dec 24**
Next Review Due	**Dec 25**
Agreed with Teacher Trade Unions and Professional Associations	**n/a**

Purpose of the policy

This policy details how Welland Park 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). See also our whole school Data Protection Policy available on our website.

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 JCQs *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.

The type of information held is as follows:

- candidate name
- access arrangement information
- 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 form
- alternative site arrangements
- attendance register copies

- candidates' scripts
- candidates' work
- certificates
- certificate destruction information
- certificate issue information
- conflicts of interest records
- entry information
- exam room incident logs
- overnight supervision information
- post-results services: confirmation of candidate consent information
- post-results services: request/outcome information
- post-results services: scripts provided by ATS service
- post-results services: tracking logs
- private candidate information
- resilience arrangements: evidence of candidate performance
- resolving timetable clashes information
- results information
- seating plans
- special consideration information
- suspected malpractice reports/outcomes
- transfer of credit information
- transferred candidate arrangements
- very late arrival reports/outcomes

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

- Awarding bodies
- Joint Council for Qualifications (JCQ)

Plus, any other organisations relevant to the centre e.g. Department for Education; Local Authority.

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

- hard copy
- email
- secure extranet site(s) – [e.g. AQA Centre Services; OCR Interchange; Pearson Edexcel Online; WJEC Secure Portal; etc.]
- any other methods as appropriate to our centre e.g. a Management Information System (MIS) provided by Capita SIMS, sending/receiving information via electronic data interchange (EDI) using A2C (to/from awarding body processing systems, etc.)

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

Section 2 – Informing candidates of the information held

Welland Park Academy ensures that candidates are aware of the information and data held by giving them access to this policy via email and via the centre's website prior to registrations/entries being 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 – 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**

Mr M Towers (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 4 – 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.

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 as and when applicable (this may include updating antivirus software, firewalls, internet browsers etc.)

Section 5 – 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.

Section 6 – Access to information

(Please refer to the ICO's 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 should be made, in the first instance, to the examinations officer examsofficer.wp@wellandparkacademy.com and ID will need to be confirmed if a former candidate is unknown to current staff.

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 Mr M Jerred (Vice Principal)/Mr M Towers (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.