

Isaac Newton Academy

# General Data Protection Regulation Policy (Exams)

2020/21

## Contents

Key Staff .....	2
Purpose of the Policy .....	2
Section 1 – Exams-Related Information.....	2
Section 2 – Informing Candidates of the Information Held.....	3
Section 3 – Hardware and Software .....	3
Section 4 – Dealing with Data Breaches .....	4
1. Containment and recovery .....	4
2. Assessment of on-going risk .....	4
3. Notification of breach .....	4
4. Evaluation and response.....	5
Section 5 – Candidate Information, Audit, and Protection Measures.....	5
Section 6 – Data Retention Periods .....	5
Section 7 – Access to Information .....	5
Third Party Access.....	5
Section 8 – Table recording candidate exams-related information held .....	0

## Key Staff

Role	Names
Head of Centre	The Principal
Exams Officer line manager (Assistant Principal (data and assessment))	Mark Crowther-Green
Data and Exams Manager	Aidan Rothnie
IT Support	Mohammed Rezwan
Data Protection Officer	Aidan Rothnie

## Purpose of the Policy

This policy details how Isaac Newton 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 General Data Protection Regulation (GDPR).

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 and 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
- Not transferred outside the European Economic Area without adequate protection

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 officer 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*.

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

- Awarding bodies
- Joint Council for Qualifications
- Department for Education
- Local Authority
- ARK Multi-Academy Trust
- The press

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

- Hard copy
- E-mail

- Secure extranet sites – e-AQA; OCR Interchange Pearson Edexcel Online; WJEC Secure Services
- Management Information System (MIS) provided by Advanced Learning sending/receiving information via Electronic Data Interchange (EDI) using 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 exams results/post-results/certificate information.

## Section 2 – Informing Candidates of the Information Held

Isaac Newton Academy ensures that candidates are fully aware of the information and data held.

All candidates are:

- Informed via centre newsletter, electronic communication, and presentations
- Given access to this policy via centre website

Candidates are made aware of the above at the start of their course of study leading to an externally accredited qualification.

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 JCQ awarding bodies process their personal data in accordance with the DPA 2018 and GDPR.

Candidates eligible for access arrangements are also required to provide their consent by signing the GDPR compliant JCQ candidate personal data consent form (*Personal data consent, Privacy Notice (AAO), and Data Protection confirmation*) 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 are protected in line with DPA & GDPR requirements.

Hardware	Protection measures
<b>Desktop computer</b>	Microsoft Windows updates and patches as released; Sophos antivirus updated daily

  

Software/online system	Protection measure(s)
<b>MIS</b>	Protected usernames and passwords; centre administrator has to approve the creation of new user accounts and determine access rights
<b>Internet browser(s)</b>	Student web filter; regularly updated firewall and anti-virus software
<b>Awarding body secure extranet sites</b>	Protected usernames and passwords; centre administrator has to approve the creation of new user accounts and determine access rights
<b>A2C</b>	Installed only on centre administrator's computer

## 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 unauthorized use
- Equipment failure
- Human error
- Unforeseen circumstances such as a fire or flood
- Hacking attack
- ‘Blagging’ offences where information is obtained by deceiving the organization who holds it

If a data protection breach is identified, the following steps will be taken:

### 1. Containment and recovery

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 recognize when someone tries to use stolen data to access accounts
- Which authorities, if relevant, need to be informed

### 2. Assessment of on-going 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 yearly.

The table below details the type of 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
- Sophos antivirus updated daily
- Microsoft Windows updates and patches as released

## Section 6 – Data Retention Periods

Details of retention periods, the actions taken at the end of the retention period, and the methods of disposal are contained in the centre's Exams Archiving Policy which is available from the centre's website.

## Section 7 – Access to Information

Current and former candidates can request access to information/data held on them by making a **subject access request** to the Data Protection Officer in writing. All requests will be dealt with within 40 calendar days.

### Third Party Access

Permission should be obtained before requesting personal information on another individual from a third-party organization.

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 in 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), 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)
- 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 centre will make reference to the ICO (Information Commissioner's Office) Education and Families <https://ico.org.uk/for-organisations/education/> information on Publishing 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	What personal/sensitive data is/may be contained in the information	Where information is stored	How information is protected	Retention period
<b>Access arrangements information</b>	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 The exams office	Secure name and password The exams office is always locked	After the deadline for EARs
<b>Alternative site arrangements</b>	Candidate name Candidate number Candidate entries Candidate tier information	MIS The exams office Alternative site	Secure name and password The exams office is always locked	After the deadline for EARs
<b>Attendance registers copies</b>	Candidate name Candidate number Candidate tier information (where applicable)	The exams office	In secure area solely assigned to exams	After the deadline for EARs
<b>Candidates' scripts</b>	Candidate name Candidate number Candidate tier information Candidate assessment data	Classrooms Staff learning rooms The exams office	Lockable cabinets within staff learning rooms and classrooms Students are forbidden from entering staff learning rooms The exams office is always locked	n/a
<b>Candidates' work</b>	Candidate name Candidate number Candidate tier information	Classrooms Staff learning rooms The exams office	Lockable cabinets within staff learning rooms and classrooms	After the deadline for EARs



Information Type	What personal/sensitive data is/may be contained in the information	Where information is stored	How information is protected	Retention period
	Candidate assessment data		Students are forbidden from entering staff learning rooms The exams office is always locked	
<b>Certificates</b>	Candidate name Candidate number Candidate DoB Unique Candidate Identifier (UCI) Qualification grades	The main reception The exams office	Lockable metal cabinet The exams office is always locked	Two years after certificate evening
<b>Certificate destruction information</b>	Candidate name Candidate number Unique Candidate Identifier	The exams office	The exams office is always locked	
<b>Certificate issue information</b>	Candidate name	The main reception	Lockable metal cabinet	
<b>Conflicts of Interest records</b>	Staff name Name of staff's close associate Details of qualifications entered	The exams office	The exams office is always locked	
<b>Entry information</b>	Candidate name Candidate number Candidate tier information (where applicable)	MIS Exams Officer's computer The exams office	Secure user name and password In secure area solely assigned to exams	
<b>Exam room incident logs</b>	Candidate name Candidate number Details of incident involving candidate(s)	The main exam venue The exams office	In possession of lead invigilator The exams office is always locked	After the deadline for EARs and/or appeals have been exhausted
<b>Invigilator and facilitator training records</b>	Invigilator name Attendance	The exams office	The exams office is always locked	After the deadline for EARs and/or appeals have been exhausted

Information Type	What personal/sensitive data is/may be contained in the information	Where information is stored	How information is protected	Retention period
<b>Overnight supervision information</b>	Candidate name Candidate number Details of overnight supervision arrangements Candidate address Candidate contact details	The exams office	The exams office is always locked	After the deadline for EARs and/or appeals have been exhausted
<b>Post-results services: confirmation of candidate consent information</b>	Candidate name Candidate number	The exams office	The exams office is always locked	After the deadline for EARs and/or appeals have been exhausted
<b>Post-results services: scripts provided by ATS service</b>	Candidate name Candidate number Qualification grades and marks Candidate answers to questions	IT network Awarding body secure extranet site Staff learning rooms Classrooms The exams office	Secure user name and password Lockable cabinets within staff learning rooms and classrooms The exams office is always locked	After the deadline for EARs and/or appeals have been exhausted
<b>Post-results services: tracking logs</b>	Candidate name Candidate number	Exams Officer's computer The exams office	Secure user name and password The exams office is always locked	After the deadline for EARs and/or appeals have been exhausted
<b>Private candidate information</b>	Candidate name Candidate number Candidate UCI Candidate ULN Candidate DoB Gender Candidate timetable	MIS Exams Officer's computer Awarding body secure extranet site The exams office	Secure user name and password The exams office is always locked	After the deadline for EARs and/or appeals have been exhausted
<b>Resolving clashes information</b>	Candidate name Candidate number Candidate UCI Candidate timetable	MIS Exams Officer's computer The exams office	Secure user name and password The exams office is always locked	After the deadline for EARs and/or appeals have been exhausted

Information Type	What personal/sensitive data is/may be contained in the information	Where information is stored	How information is protected	Retention period
<b>Results information</b>	Candidate name Candidate number Candidate UCI Candidate ULN Candidate DoB Qualification grades	MIS Exams Officer's computer The exams office Awarding body secure extranet site Teacher reports	Secure user name and password In secure area solely assigned to exams Lockable cabinets within staff learning rooms and classrooms	
<b>Seating Plans</b>	Candidate name Candidate number Candidate UCI	Exams Officer's computer The exams office Exams venues	Secure user name and password The exams office is always locked	After the deadline for EARs and/or appeals have been exhausted
<b>Special consideration information</b>	Candidate name Candidate number Candidate UCI Candidate DoB Medical details (if applicable) Safeguarding information (if applicable)	Awarding body secure extranet site The exams office Pastoral leader	Secure user name and password The exams office is always locked	After the deadline for EARs and/or appeals have been exhausted
<b>Suspected malpractice reports/outcomes</b>	Candidate name Candidate number Candidate UCI Qualification codes Personal details as pertaining to the incident Evidence	Exams Officer's computer The exams office Awarding body malpractice dept.	Secure user name and password The exams office is always locked Email correspondence with awarding body	
<b>Transferred candidate information</b>	Candidate name Candidate number Candidate UCI Candidate ULN Entry codes Tier information (where applicable)	The exams office Awarding body extranet Previous school	Secure user name and password The exams office is always locked Email correspondence with previous school	

Information Type	What personal/sensitive data is/may be contained in the information	Where information is stored	How information is protected	Retention period
<b>Very late arrival reports/outcomes</b>	Candidate name Candidate number Entry codes	The exams office Awarding body	Secure user name and password Email correspondence with awarding body The exams office is always locked	

Reviewed June 2020