Ark Putney Academy

General Data Protection Regulation policy (Exams)

2021/22

Key staff involved in the General Data Protection Regulation policy

Role	Name(s)
Head of centre	*Alison Downey*
Exams officer	*Sue Lambird*
Exams Officer line manager (Senior Leader)	*Colin Shallcross*
Data Protection officer	*Colin Shallcross*
IT manager	*Dardan Grajqevci*
Data manager	*Alex Johnson*

Purpose of the policy

This policy details how Ark Putney 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).

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 these *General Regulations* 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. (JCQ General Regulations for Approved Centres (section 6.1) **Personal data**)

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 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 – 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
- email

- Secure extranet site(s) – e-AQA; OCR Interchange; Pearson Edexcel Online; WJEC Secure services
- Management Information System (MIS) provided by Bromcom
- Academy Website
- sending/receiving information via electronic data interchange (EDI) using A2C (https://www.jcq.org.uk/about-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, special consideration requests and exam results/post-results/certificate information.

Section 2 – Informing candidates of the information held

Ark Putney Academy ensures that candidates are informed **on request** of the information and data held.

All candidates are:

- given access to this policy via exams office and 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 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 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 is protected in line with DPA & GDPR requirements.

Hardware	Protection measures
Desktop Computer	Microsoft Windows updates and patches as released; Sophos antivirus updated daily, encrypted via bitlocker.

Software/online system	Protection measure(s)
Bromcom MIS System	Protected usernames and passwords; centre administrator has to approve the creation of new user accounts and determine access rights

Internet browser	Student web filter: regularly updated firewall and anti-virus software, run through LGFL.
Awarding body secure extranet sites	Protected usernames and passwords; exams officer has to approve the creation of new user accounts and determine access rights
A2C	Installed only on exams officer'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 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 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 anything 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 has been 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.

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
- Sophos antivirus updated daily
- Microsoft Windows updates and patches as released
- Staff passwords changed every 3 months

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 office.

Section 7 – Access to information

Current and former candidates can request access to results information/data held on them by making to the Exams Officer or Data Manager in writing/email. All requests will be dealt with within 30 calendar days.

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, is 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), 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

When considering publishing exam results, the Ark Putney will refer to the ICO (Information Commissioner's Office) Education and Families https://ico.org.uk/for-organisations/education/ Can schools give my exam results to the media for publication?

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 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 in SEN department	Secure user name and password In secure area solely assigned to SEN staff	
Attendance registers copies	Candidate name Candidate number Subject/tier (where applicable) Information	Exams Office Files	In exams office	1 Year
Candidates' scripts	Candidate name, Candidate number Subject/tier (where applicable) Information	Exams Office	In secure area solely assigned to exams Lockable metal filing cabinet	
Certificates	Candidate name Candidate number/UCI	Exams Office	Certificates returned to the school will be kept in a lockable metal filing cabinet	

Information type	What personal/sensitive data is/may be contained in the information	Where information is stored	How information is protected	Retention period
	Candidate DoB Qualification grades			
Entry information	Candidate name, Candidate number Subject/tier Information	Exams office files	The exams office is always locked	1 Year
Exam room incident logs	Candidate name Candidate number Details of incident involving candidate(s)	Exams office files	The exams office is always locked	1 Year
Invigilator and facilitator training records	Invigilator name	Exams office files	The exams office is always locked	ongoing
Post-results services: confirmation of candidate consent information	Candidate name, Candidate number Subject/tier Information	Exams office files	The exams office is always locked	1 Year
Post-results services: requests/outcome information	Candidate name Candidate number/UCI Candidate DoB Subject/subject code Qualification grade	Exams office files	Secure user name and password The exams office is always locked	1 Year
Post-results services: scripts provided by ATS service	Candidate name Candidate number Qualification grades and marks	Exams Office Awarding body secure extranet	The exams office is always locked	1 Year

Information type	What personal/sensitive data is/may be contained in the information	Where information is stored	How information is protected	Retention period
	Candidate answers	Staff learning rooms Classrooms	Secure user name and password Lockable cabinets within staff learning rooms and classrooms	
Private candidate information	N/A			
Resolving timetable clashes information	Candidate name Candidate number/UCI Candidate DoB Candidate timetable	MIS Exam office files	Secure user name and password The exams office is always locked	1 Year
Results information	Candidate name Candidate number/UCI Candidate DoB Qualification grades and marks	MIS Awarding body secure extranet Exam Office Files	Secure user name and password The exams office is always locked	10 Years
Special consideration information	Candidate name Candidate number/UCI Candidate DoB Medical details Safeguarding information	Awarding body secure extranet Exam Office Files SEN department	Secure user name and password The exams office is always locked	1 Year
Suspected malpractice reports/outcomes	Candidate name Candidate number/UCI Candidate DoB	Awarding body secure extranet Exam Office Files	Awarding body secure extranet Exam Office Files	1 Year

Information type	What personal/sensitive data is/may be contained in the information	Where information is stored	How information is protected	Retention period
	Personal details as pertaining to the incident Evidence			
Transfer of credit information	Candidate name Candidate number/UCI/ULN Entry codes	Awarding body secure extranet Exam Office Files	Secure user name and password The exams office is always locked Exams officer email	1 Year
Transferred candidate arrangements	Candidate name Candidate number/UCI/ULN Entry codes	Awarding body secure extranet Exam Office Files	Secure user name and password The exams office is always locked Exams officer email	1 Year
Very late arrival reports/outcomes	Candidate name Candidate number/UCI	Awarding body secure extranet Exam Office Files	Awarding body secure extranet Exams office is always locked	1 Year