Data Protection Policy (Exams)

Agreed date: Autumn 2023

Review date: Autumn 2024

Responsibility of: Exams Manager

Purpose of the policy

This policy details how Reepham High School and College (RHSC), in relation to exams management and administration, ensures compliance with the regulations as set out by the Data Protection Act 2018 (DPA) 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* (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 and UK GDPR, all candidates' exam information – even that which is not classified as personal or sensitive – is covered under this policy.

This policy will be reviewed annually

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
- ▶ Department for Education
- ▶ Norfolk Local Authority
- ▶ Synergy Trust (Multi Academy Trust)
- ▶ Local press

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

- ▶ hard copy
- ▶ email

- ► secure extranet site(s): - eAQA; AQA Centre Services, OCR Interchange; Pearson Edexcel Online; WJEC Secure services
- ► Management Information System (MIS), provided by SIMs, for sending/receiving information via electronic data interchange (EDI) using A2C (https://www.jcq.org.uk/about-a2c) to and 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

RHSC ensures that candidates and parents are fully aware of the information and data held.

All candidates/parents are:

- ► given access to this policy via the school/college websites
- ► given information via privacy notices that are signed and held on file. The school's privacy notice document is available on the school/college website.

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). This is in the Exams Handbook which is sent to all students taking external exams.

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 approved 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	Warranty expiry
Exams Office PCs x 2 (Exams Manager and Exams Assistant)	PCs are password protected. Passwords must contain a mix of upper and lower case, letters and numbers and must be changed termly. Exams Office is secured with a code key, known to 4 members of staff. Antivirus protection is kept up to date and runs a weekly scan to check for security breaches	N/A

Software/online system	Protection measure(s)

Management information system (SIMs)	Network access is password protected. Passwords must contain a mix of upper and lower case, letters and numbers and must be changed termly. Access to the Exams function is limited to the Exams Manager, Exams Assistant, Data Manager and IT Manager.
Local network storage (Y drive, exams folder)	Network access is password protected. Passwords must contain a mix of upper and lower case, letters and numbers and must be changed termly. The exams folder is only accessible to the Exams Manager and Exams Assistant.
Awarding bodies' secure extranet sites	Password protected. Exams Manager is the administrator for all the awarding bodies' websites and ensures correct access is applied to all users. Plus, annual "spring clean" before results days.
A2C – transport application for exam entries and results	Can only be accessed on Exams Manager's PC and laptop both of which are password protected. Passwords must contain a mix of upper and lower case, letters and numbers). Passwords must be changed termly.

Section 4 – Contingency procedure for 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 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 5 – Candidate information 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 in section 8 details the type of candidate exams-related information held, and how it is managed, stored and protected.

Section 6 – Data retention periods/archiving

Details of retention periods, the actions taken at the end of the retention period, archiving and method of disposal are contained in Section 8 of this document, and also in the Exams Archiving Policy

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 Exams Manager initially by email. An ID verification will need to take place using photo ID before any data can be released.

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.

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 (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

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request or have given their consent. Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at our school may be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.Children aged 12 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at our school may not be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

Publishing exam results

When considering publishing exam results, RHSC 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?

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**)

Information type	What personal/sensitive data is/may be contained in the information	Where information is stored	How information is protected	Retention period and action at end of 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 and teachers' feedback Medical evidence Samples of work	Access Arrangements Online MIS Lockable metal filing cabinet	Secure username and password Secure username and password In secure area solely assigned to SEN	**Stored by exams:** Returned to SENCo as records holder at the end of the candidate's final exam **Stored by SENCo**: 5 years from years 9-13, then files sent to archives.
Alternative Site Arrangements	Candidate name, DOB, details of exams taken. Could include home address	CAP and Exams Office	Secure username and password Exams Office is locked when not in use	Retained until the deadline for EARs or resolution of any enquiries, appeals, malpractice whichever is longer. Confidential destruction thereafter.
Attendance registers copies	Candidate name Exam number	MIS Metal filing cabinet in secure store	Secure username and password Keycode entry to secure store	Retained until the deadline for EARs or resolution of any enquiries, appeals, malpractice whichever is longer. Confidential destruction thereafter.
Candidates' scripts	Candidate name Exam number	Locked safe in secure store	Safe key in coded key safe. Keycode entry to secure store	Scripts are kept securely if necessary, to the next day after the

Information type	What personal/sensitive data is/may be contained in the information	Where information is stored	How information is protected	Retention period and action at end of retention period
	Candidate's work			exam when they are sent using the yellow label Parcelforce service
Candidates' work (NEA and coursework)	Candidate name Exam number Candidate's work	Immediately returned to subject leaders	Store securely by subject leaders	Retained until the deadline for EARs or resolution of any enquiries/appeals/malpractice whichever is longer. Returned to candidates thereafter
Certificates	Candidate name Candidate DOB UCI/ULN Grades achieved	Metal filing cabinet in secure store	Key code entry to secure store. Candidates must sign for certificates and produce ID if they do not attend Awards Evening.	Unclaimed certificates are kept for 2 years and then confidentially destroyed noting details on certificate destruction log.
Certificate destruction log	Candidate name Date of exams, boards and subjects	Metal filing cabinet in secure store	Key code entry to secure store	Retained for 5 years from the date of the certificate destruction then confidentially destroyed
Certificate issue information	Candidate name Year sitting exams	Metal filing cabinet in secure store	Key code entry to secure store	Retained for 5 years then confidentially destroyed.
Conflicts of Interest Information	Details of centre staff taking or with close relations/friends taking exams, names and exam details.	Exams Office	Exams Office is locked when not in use	Retained until the deadline for EARs or resolution of any enquiries, appeals, malpractice whichever is longer. Confidential destruction thereafter.
Entry information and SoE	Candidate name Candidate DoB Exam number/UCI/ULN	File in Exams Office	Exams Office is locked when not in use	Retained until the next year's entries are made, then confidentially destroyed

Information type	What personal/sensitive data is/may be contained in the information	Where information is stored	How information is protected	Retention period and action at end of retention period
	Registration group Exam entries			
Exam room incident logs	Candidate name Exam number Personal incidents/issues	Metal filing cabinet in secure store	Key code entry to secure store	Retained for 1 year then confidentially destroyed
Overnight supervision information	Candidate name Exam number Reason for timetable variation	In file in the Exams Office	Exams Office is locked when not in use	Retained for 1 year then confidentially destroyed
Post-results services: confirmation of candidate consent information	Candidate name, Exam number Exam query details	In file in the Exams Office	Exams Office is locked when not in use	For at least 6 months after outcome received (EAR) or date of consent (ATS) then confidentially destroyed
Post-results services: requests/outcome information	Candidate name Exam number Query details and outcome	In file in the Exams Office and Data Office	Exams Office is locked when not in use	Retained for 1 year
Post-results services: scripts provided by ATS service	Candidate name Exam number Exam script	Given to HoD or student immediately	HoD keep secure	Kept secure until no longer needed then confidentially destroyed
Post-results services: tracking logs	Candidate name, Exam number Subject/level of query	In file in the Exams Office	Exams Office is locked when not in use	Retained for 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 and action at end of retention period
Resolving timetable clashes information	Candidate name Exam number Exam clash details	In file in the Exams Office	Exams Office is locked when not in use	Retained until the next year's entries are made, then confidentially destroyed
Results information	Candidate name Exam number/UCI/ULN DOB Grades	Metal filing cabinet in secure store and Data Office	Key code entry to secure store	Records for current year plus previous 6 years
Seating plans	Candidate name Exam number Access arrangements	Metal filing cabinet in secure store	Key code entry to secure store	Retained for 1 year, then confidentially destroyed
Special consideration information	Candidate name Exam number Personal details of special consideration application	In file in the Exams Office	Exams Office is locked when not in use	Retained until the deadline for EARs or resolution of any appeals or malpractice whichever is longer.
Suspected malpractice reports/outcomes	Candidate/member of staff name Exam number Malpractice details	Metal filing cabinet in secure store	Key code entry to secure store	Retained for 3 years
Transferred candidate arrangements	Candidate name Exam Number DoB	In file in the Exams Office	Exams Office is locked when not in use	Retained until arrangements confirmed by the awarding body

Information type	What personal/sensitive data is/may be contained in the information	Where information is stored	How information is protected	Retention period and action at end of retention period
Very late arrival reports/outcomes	Candidate name Exam number Details of late arrival	Metal filing cabinet in secure store	Key code entry to secure store	Retained for 3 years