DATA PROTECTION POLICY (Exams)

2022/23

This policy is reviewed annually to ensure compliance with current regulations

Approved/reviewed by	
Lauren Calver	
Date of next review	20/09/23

Key staff involved in the policy

Role	Name(s)
Head of centre	Sian Thomas
Exams officer	Lauren Calver

Contents

Purpose of the policy

This policy details how Ancora House 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 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 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 below.

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

- Awarding bodies
- Joint Council for Qualifications (JCQ)
- DFE
- Cheshire and Wirral Partnership NHS trust

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

- hard copy
- email
- secure extranet site(s) – AQA Centre Services; Pearson Edexcel Online;
- sending/receiving information via electronic data interchange (EDI) using A2C (https://www.jcq.org.uk/about-a2c)

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

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

All candidates are:

- informed via their examinations pack they receive after entries go in
- given access to this policy via written request

Candidates are made aware of the above after receiving their examinations pack they receive after entries go in

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* 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 – 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
Pen drive /USB with word processed script on	July 2022 – Pen drive will be securely labelled and kept in the secure storage/ exams store	N/A

Software/online system	Protection measure(s)
Awarding Body secure sites	Limited number of staff able to access the sites, check annually that access is appropriate Only access websites on school encrypted devices
School Secure Server	Data backed up overnight, access only via VPN or whilst on school site, only SLT have VPN access.
SIMS MIS system	Data backed up by server overnight. System can only be accessed via school encrypted device as it is not cloud based. School staff reminded to keep passwords private and secure

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

The School Business Manager and the schools DPO within CWAC council 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, 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 annually.

The table below details the type of candidate exams-related information held, and how it is managed, stored and protected

Protection measures may include:

- secure drive accessible only to selected staff
- information held in secure area
- updates undertaken every 3months (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 school server.

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 officer in writing confirming the year when they sat examinations at the school and home school they were entered with (if they are a transferred candidate)

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 the HOC 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 written request is accompanied with permission from the candidate and appropriate evidence (where relevant), to verify the ID of both parties, and reasoning behind the request.

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 not disclose information with parents if the candidate requests us not to , the centre will always consult the candidate before disclosing information relating to exams.

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, Ancora House School 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?

As Ancora House 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 the HOC 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.

The majority of the cohort of the school are transferred candidates, the school will request copies of transferred candidates results for our internal data and tracking purposes, which will be summarised on the website.

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	AA online if processed by AHS Secure Server Exams file (locked in exam store)	Secure school server restricted access Store Stored in secure exams store , limited key holders and FOB access	Year of exam plus 6
Alternative site arrangements		Addresses of sites and candidate information , Name , DOB, Gender	CAP portal Exam file	Store Stored in secure exams store , limited key holders and FOB access	Year of exam plus 6
Attendance registers copies		Name , candidate and centre number	Exam paper file	Store Stored in secure exams store , limited key holders and FOB access	Year of exam plus 6
Candidates' scripts		Name , candidate and centre number	Exam paper file	Store Stored in secure exams store , limited key holders and FOB access	Year of exam plus 6

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
Candidates' work		Name , candidate and centre number	Exam paper file	Secure storage cupboard	Year of exam plus 6
Centre consortium arrangements for centre assessed work		Name , candidate and centre number DOB	Exam paper file	Store Stored in secure exams store , limited key holders and FOB access	Year of exam plus 6
Certificates		Name , candidate and centre number, DOB	Exam paper file	Secure storage cupboard	Year of exam plus 6
Certificate issue information		Name, results, centre and candidate number Name of staff member issuing	Electronic and paper exam files	Store Stored in secure exams store , limited key holders and FOB access Stored on restricted area on secure server d in secure exams store , limited key holders and FOB access	Year of exam plus 6
Entry information		Name, dob, UCI, Candidate and centre number ULN	Electronic and paper exam files Secure interchange of awarding body	Store Stored in secure exams store , limited key holders and FOB access Stored on restricted area on secure server d in secure exams store , limited key holders and FOB access Exam sites have limited users with secure passwords	Year of exam plus 6

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
Exam room incident logs		Name of candidate, centre number, candidate number Name of invigilator	paper exam files	Store Stored in secure exams store , limited key holders and FOB access Stored on restricted area on secure server d in secure exams store , limited key holders and FOB access	Year of exam plus 6
Invigilator and facilitator training records		Staff member name as well as invigilators details	Electronic and paper exam files	Stored in secure exams store , limited key holders and FOB access Stored on restricted area on secure server	Year of exam plus 6
Post-results services: confirmation of candidate consent information		Candidate name and number Centre name and number Results data	Electronic and paper exam files	Stored in secure exams store , limited key holders and FOB access Stored on restricted area on secure server	Year of exam plus 6
Post-results services: requests/outcome information		Candidate name and number Centre name and number Results data	Electronic and paper exam files	Stored in secure exams store , limited key holders and FOB access Stored on restricted area on secure server	Year of exam plus 6

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
Post-results services: scripts provided by ATS service		Candidate name and number Centre name and number Results data	Electronic and paper exam files	Stored in secure exams store , limited key holders and FOB access Stored on restricted area on secure server	Year of exam plus 6
Post-results services: tracking logs		Candidate name and number Centre name and number Results data	Electronic and paper exam files	Stored in secure exams store , limited key holders and FOB access Stored on restricted area on secure server	Year of exam plus 6
Results information		Candidate name and number Centre name and number Results data	Electronic and paper exam files	Stored in secure exams store , limited key holders and FOB access Stored on restricted area on secure server	Year of exam plus 6
Seating plans		Candidate name , number , Centre name and number Access arrangements	Electronic and paper exam files	Stored in secure exams store , limited key holders and FOB access Stored on restricted area on secure server	Year of exam plus 6
Special consideration information		Candidate name , number , Gender, DOB	On secure exams interchange sites Electronic and paper exam files	Store Stored in secure exams store , limited key holders and FOB access Stored on restricted area on secure	Year of exam plus 6

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
				server d in secure exams store , limited key holders and FOB access Exam sites have limited users with secure passwords	
Suspected malpractice reports/outcomes		Candidate name , number, gender	On secure exams interchange sites Exam paper and electronic files	Exam sites have limited users with secure passwords Stored in secure exams store , limited key holders and FOB access Stored on restricted area on secure server	Year of exam plus 6
Transferred candidate arrangements		Names of candidates and centre, centre and candidate number	Examination's file and electronic file on server	Stored in secure exams store , limited key holders and FOB access Stored on restricted area on secure server	Year of exam plus 6
Very late arrival reports/outcomes		Candidate name and centre number	Examinations file	Stored in secure exams store , limited key holders and FOB access	Year of exam plus 6

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