

DATA PROTECTION POLICY (Exams)

2022/23

This policy is reviewed annually to ensure compliance with current regulations

Approved/reviewed by	
Date of next review	

Key staff involved in the policy

Role	Name(s)
Head of centre	Steve Brogan
Exams officer	Jackie Morris
Senior leader(s)	Steve Brogan – Christina Hartharn – Dave Warden – Kerry Boddice – Kim McDermott
IT manager	James Reeks
Data manager	Claire Marr

Contents

Key staff involved in the policy	2
Purpose of the policy	4
Section 1 – Exams-related information.....	4
Section 2 – Informing candidates of the information held	5
Section 3 – Hardware and software.....	5
Section 4 – Dealing with data breaches.....	6
Section 5 – Candidate information, audit and protection measures	7
Section 6 – Data retention periods	7
Section 7 – Access to information.....	8

Purpose of the policy

This policy details how Saint John Houghton Catholic Voluntary 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 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)
- Department for Education;
- Local Authority;
- Saint Ralph Sherwin Multi Academy Trust;

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

- hard copy
- email
- secure extranet site(s) - AQA Centre Services; OCR Interchange; Pearson Edexcel Online; WJEC Secure Website;
- a Management Information System (MIS) provided ESS SIMS) 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

Saint John Houghton Catholic Voluntary Academy ensures that candidates are fully aware of the information and data held.

All candidates are:

- informed via student briefing, centre news update, electronic communication
- given access to this policy via centre website, written request,
- Candidates are made aware of the above at the start of a course leading to a vocational qualification, or, where candidates are following GCSE qualifications, when the entries are submitted to awarding bodies for processing.

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
Desktop computers	Purchase date: Unknown Checked Termly by ICT team adhering to ICT Policy. Checked for functionality and general operability, Virus scanned on schedule & constantly monitored for threats. Data is only storable on encrypted network drives. All applications commonly used by staff and pupils are as up to date as they can be. Protected by up to Date Sophos Endpoint Protection. Operating systems automatically install latest Windows updates & security updates	N/A All Devices out of warranty
Laptop computers	Purchase date: Unknown Checked Termly by ICT team adhering to ICT Policy. Checked for functionality and general operability, Virus scanned on schedule & constantly monitored for threats. Data is only storable on encrypted network drives. All applications commonly used by staff and pupils are as up to date as they can be. Protected by up-to-Date Sophos Endpoint Protection. Operating systems automatically install latest Windows updates & security updates	N/A All Devices out of warranty

Software/online system	Protection measure(s)
Username/Passwords for Computers	Only authorised staff have access to the ICT systems. Approved & Created by ICT Team Passwords require a mix of upper/lower case and numbers and require changing on a scheduled basis. Access rights manually determined by ICT staff. Based on the principle of least privilege. Giving users the minimum permissions they need to carry out their required role.
Web Browsers – MS Edge & Google Chrome	Both browsers set to automatically update as newer versions are released, ensuring that they incorporate the latest fixes. Web filtering provided by 3d Party – Ekte
A2C Software	Latest version installed
SIMS Connected	Cloud hosted SIMS Connected in use at the school. Only approved staff have access to SIMS & are assigned the roles needed to carry out their job roles. Each user requires setting up Multi Factor Authentication to log in, to protect their account.
Go4Schools	Web based software that is used to record exam results, analyse data and produce reports. Initial access to G4S is assigned to students, parents and staff based on the information in our MIS. Staff permissions are linked to roles and are manually updated on a regular basis.
ExamWritePad	Word processing Software used when conducting exams on PCs/Laptops to comply with conditions set by each exam board.

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

John Walker, 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, 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 regularly by ICT and SRSCMAT.

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
- updates undertaken as browsers set to automatically update as newer versions are released (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 and SRSCMAT Information and Records Retention policy which is available/accessible from exams officer and SRSCMAT website.

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 Data Protection Officer or exams officer in writing/email 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 Head of Centre/DSL 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), 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

Saint John Houghton Catholic Voluntary Academy will publish exam results to the media or within the centre (e.g. on an honours board) in line with the following principles:

- Refer to guidelines as published by the Joint Council for Qualifications
- Follow SRSCMAT guidelines for publishing results
- Act fairly when publishing results, and where people have concerns about their or their child's information being published, taking those concerns seriously
- Ensure that all candidates and their parents/carers are aware as early as possible whether examinations results will be made public and how this will be done
- Explain how the information will be published. For example, if results will be listed alphabetically, or in grade order

As Saint John Houghton Catholic Voluntary Academy 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 Head of Exams, 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.

