

Data Protection Policy

(Exams)

2020/21

This policy is reviewed annually to ensure compliance with current regulations

Approved/reviewed by	
Mr A. Shaw	
Date of next review	October 2021

Key staff involved in the policy

Role	Name(s)
Head of centre	Mr G. Langston-Jones
Exams officer	Mrs J. Haddock
Senior leader(s)	Mr A. Shaw
IT manager	Mr A. Dicken
Data manager	Mr J. Bates

Purpose of the policy

This policy details how Nether Stowe 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 General Data Protection Regulation (GDPR).

At the date of reviewing these regulations, although the UK has left the European Union the General Data Protection Regulation still has a direct effect within the UK (JCQ's [General Regulations for Approved Centres](#) (GR, 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
- 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 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 (JCQ)
- [insert (by listing) any other organisations as relevant to your centre e.g. Department for Education; Local Authority; Multi Academy Trust; Consortium; the Press; etc.]

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

- hard copy
- email
- secure extranet site(s) – Exam Boards: eAQA; OCR Interchange; Pearson Edexcel Online; WJEC Secure Website
- Management Information System (MIS) provided by Capita SIMS) 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 exam results/post-results/certificate information.

Section 2 – Informing candidates of the information held

Nether Stowe School ensures that candidates are fully aware of the information and data held.

All candidates are:

- given access to this policy via school website or written request

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 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 is protected in line with DPA & GDPR requirements.

Hardware	Date of purchase and protection measures	Warranty expiry
Network Servers	Sophos Antivirus	TBC (ATLP source)
Desktop Computer	Smoothwall Filtering Visigo	TBC (ATLP source) TBC (ATLP source)

Software/online system	Protection measure(s)
MIS (Sims)	Setting User Accounts with permissions and access restrictions
Intranet	Protected usernames and passwords; rules for password setting (use of a mix of upper/lower case letters and numbers); rules for regularity of password changing; centre administrator has to approve the creation of new user accounts and determine access rights; regular checks to Firewall/Antivirus software

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

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

1. Containment and recovery

Our Data Protection Officer and IT manager will lead an investigation into 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:

- password protected area on the centre's intranet
- secure drive accessible only to selected staff
- information held in secure area
- updates undertaken every month (updating antivirus software, firewalls, internet browsers)

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 on the school website

Section 7 – Access to information

The GDPR gives individuals the right to see information held about them. This means individuals can request information about them and their exam results, 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/email.

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.

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 results have been announced, 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

Candidates' personal data will not be shared with a third party unless written permission is obtained. The request must be accompanied with appropriate evidence (where relevant), to verify the ID of both parties.

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. The centre's Data Protection Officer will confirm the status of these agreements and approve/reject any requests.

Section 8: Table recording candidate exams-related information held

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	Secure user name and password In secure area solely assigned to SENco	5 years
Attendance registers copies	Candidate name	Lockable metal filing cabinet	In secure area solely assigned to Exams	2 Years
Certificates	Candidate name	Lockable metal filing cabinet	In secure area solely assigned to Exams	5 Years
Certificate destruction information	Candidate name	Lockable metal filing cabinet	In secure area solely assigned to Exams	5 Years
Certificate issue information	Candidate name	Lockable metal filing cabinet	In secure area solely assigned to Exams	5 Years
Entry information	Candidate name Candidate DOB Candidate Gender	Lockable metal filing cabinet	In secure area solely assigned to Exams	2 Years
Exam room incident logs	Candidate Name	Lockable metal filing cabinet	In secure area solely assigned to Exams	2 Years
Invigilator training records	Staff Name	Lockable metal filing cabinet	In secure area solely assigned to Exams	2 Years
Post-results services: confirmation of candidate consent information	Candidate Name	Lockable metal filing cabinet	In secure area solely assigned to Exams	2 Years

Post-results services: requests/outcome information	Candidate Name	Lockable metal filing cabinet	In secure area solely assigned to Exams	2 Years
Post-results services: scripts provided by ATS service	Candidate Name	Lockable metal filing cabinet	In secure area solely assigned to Exams	2 Years
Post-results services: tracking logs	Candidate Name	Lockable metal filing cabinet	In secure area solely assigned to Exams	2 Years
Resolving timetable clashes information	Candidate Name	Lockable metal filing cabinet	In secure area solely assigned to Exams	2 Years
Results information	Candidate Name Candidate DOB	Lockable metal filing cabinet	In secure area solely assigned to Exams	2 Years
Seating plans	Candidate Name	Lockable metal filing cabinet	In secure area solely assigned to Exams	2 Years
Special consideration information	Candidate Name Candidate DOB	Lockable metal filing cabinet	In secure area solely assigned to Exams	2 Years
Suspected malpractice reports/outcomes	Candidate Name	Lockable metal filing cabinet	In secure area solely assigned to Exams	2 Years
Very late arrival reports/outcomes	Candidate Name	Lockable metal filing cabinet	In secure area solely assigned to Exams	2 Years