pipers corner SCHOOL

Examination Data Protection Policy

This policy was reviewed in: October 2023
This policy is due to be reviewed in: October 2024

Key staff involved in the policy

Role	Name(s)
Head of Centre	**Helen Ness-Gifford, Headmistress**
Examinations Officer	**Shula Hodge**
Senior Leader(s)	**Caroline Derbyshire, Deputy Head Academic**
IT Manager	**Andrew Bryson**
MIS Data Manager	**Clare Over**
GDPR Co-ordinator	**Jason Clarke, Bursar**

Contents

The purpose of the policy

This policy details how Pipers Corner School, in relation to examinations 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 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 examination 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' examination information – even that which is not classified as personal or sensitive – is covered under this policy.

Section 1 - Examination related information

There is a requirement for the Examinations Office(r) to hold examination-related information on candidates taking external examinations. For further details on the type of information held please refer to Section 5.

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

- Awarding bodies
- Joint Council for Qualifications (JCQ)

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

- hard copy
- email (activating encryption security settings)
- secure extranet site(s) (including secure cloud services as required)
- Management Information System (MIS) 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 examination entries, access arrangements, the conduct of examinations and non-examination assessments, special consideration requests and examination results/post-results/certificate information.

Section 2 – Informing candidates of the information held

Pipers Corner School ensures that candidates are fully aware of the information and data held.

All candidates are:

- informed via electronic communication
- given access to this policy via written request and on the School Learning Platform

Candidates are made aware of the above where candidates are following GCE and 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 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
2 desktop computers connected to the school network. Access to the devices is via username and password combination. Two factor authentication is used where appropriate. Laptops are encrypted.	Examination Office devices were initially installed Summer 2014. The School has a replacement policy to replace kit of a certain age. They are reviewed annually to ensure that they are fit for purpose. All school devices have Endpoint antivirus and other security features installed on the device. They sit behind a complex network, filtering and firewall solution. Email is filtered via an antispam solution.	N/A

Software/online system	Protection measure(s)
Staff use Office 365 suite of products. Web services are accessed via Google Chrome browser. The school's MIS is iSAMS which has a purpose designed examinations module.	iSAMS and Office 365 employ two factor authentication. Physical devices are inside locked room and use Active Directory authentication and security. Data stored on network areas is stored in server room 1 (next to IT Services) and backed up daily to server room 2 (next to music). Data stored on O365 is backed up to external backup service.

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
- 'blagging' offences where information is obtained by deceiving the organisation who holds it
- cyber-attacks including ransomware attacks

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

1. Containment and recovery

The School Bursar will lead on investigating the breach, supported by the Assistant Head Digital Learning and IT Manager.

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' examination-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 by the Bursar.

Appendix 1 details the type of candidate examination-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
- regular updates undertaken (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 School's Information and Records Retention Policy which is available on SharePoint, and the Centre's Examination Archiving Policy which is available/accessible from the Examination Office.

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 examination 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 examination questions.

Requesting examination information
Requests for examination information can be made to the Bursar in writing.

The GDPR does not specify an age when a child can request their examination 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 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 examination information before examination results have been published, a request will usually 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 examination results have been published, the individual will usually receive a response within one month of their request.

In complex cases of Subject Access Request, the timeframe for response may be extended by up to a further two months beyond the timeframes quoted above.

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.

Publishing examination results

Pipers Corner School will publish examination 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
- 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 Pipers Corner 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 Deputy Head Academic, who will consider the objection before making a decision to publish and reply with a good reason to reject the objection to publish the examination results.

Appendix 1 Table recording candidate examination-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	Excel spreadsheet of student names **Communication regarding access arrangements**	**Candidate Number, Year, Surname, Forename, Extra Time %, Processor, Notes, Examination Account** Managed by the school's Individual Learning department.	Academic section of SharePoint In school MIS and Individual Learning files.	Only available to academic staff to support testing Individual user access rights.	**Continuously updated so only shows current students.** **In line with other school SEN data.** **In line with the Examination Archiving Policy and the School's Information and Records Retention Policy, Access arrangements information will ultimately be passed on to the Head of Centre office once the student has taken their final examination at the School and has left the School.**

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
Attendance registers copies		Candidate name Candidate number Candidate DOB	In secure office	In secure office	6 months
Candidates' scripts			In secure office	In secure office	6 months
Candidates' work			In secure office	In secure office	6 months
Certificates			In secure office	In secure office	12 months
Conflicts of interest records			In secure office	In secure office	6 months
Entry information			In secure office	In secure office	6 months
Examination room incident logs			In secure office	In secure office	6 months
Invigilator and facilitator training records		Candidate name Candidate number Candidate DOB	In secure office	In secure office	6 months
Overnight supervision information			In secure office	In secure office	6 months
Post-results services: confirmation of candidate consent information			In secure office	In secure office	6 months
Post-results services: requests/outcome information			In secure office	In secure office	6 months
Post-results services: scripts provided by ATS service			In secure office	In secure office	6 months

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: tracking logs			In secure office	In secure office	6 months
Private candidate information			In secure office	In secure office	6 months
Resolving timetable clashes information			In secure office	In secure office	6 months
Results information			In secure office	In secure office	6 months
Seating plans			In secure office	In secure office	6 months
Special consideration information			In secure office	In secure office	6 months
Suspected malpractice reports/outcomes		Candidate name Candidate number Candidate DOB	In secure office	In secure office	6 months
Transferred candidate arrangements			In secure office	In secure office	6 months
Very late arrival reports/outcomes			In secure office	In secure office	6 months