Peacehaven Community School

GDPR
Exams Policy

Head of Centre	**Rachel Henocq**
Date	**September 2022**
Date for Review	**September 2023**
Responsibility for Review	**Head of Centre**

The key staff involved in the General Data Protection Regulation exam policy at Peacehaven Community School (PCS) are:

- Head of Centre
- Exams Officer
- Deputy Headteacher overseeing exams
- Data Protection Officer
- IT Manager

Purpose of the policy

This policy details how PCS, 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).

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.

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 the *Candidate information, audit and protection measures* section.

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

- Awarding bodies
- Joint Council for Qualifications

- Any other organisations as relevant to this 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) – e.g. AQA Centre Services; OCR Interchange; Pearson Edexcel Online; WJEC Secure services; NCFE Portal
- a Management Information System (MIS) provided by Bromcom sending/receiving information via electronic data interchange (EDI) using A2C (https://www.jcq.org.uk/about-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.

Informing candidates of the information held

PCS ensures that candidates are fully aware of the information and data held.
All candidates are given access to this policy via the centre website.
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.

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
Various Windows Desktops	Various purchase dates. All Windows machines at the school are subject to persistent security scanning and checks via network-wide deployment of Sophos security software. This is installed at both server and client levels. Regular checks from IT staff. Cannot access hardware or network without account credentials (username and password).	Various

Various Windows Laptops	Various purchase dates. All Windows machines at the school are subject to persistent security scanning and checks via network-wide deployment of Sophos security software. This is installed at both server and client levels. Regular checks from IT staff. Cannot access hardware or network without account credentials (username and password).	Various
Various Chromebooks	Various purchase dates. All Chromebooks are subject to the security features built into Chrome OS which are constantly updated by Google. All data is cloud based in Google's servers so please refer to Google's security and protection policies. Regular checks from IT staff. Cannot access hardware or data without @swale.at account credentials (username and password).	Various

Software/online system	Protection measure(s)
Local Network/Windows/Active Directory	Managed by onsite and offsite IT staff (including all administrator functions e.g. account creation, setting access rights, health check and maintenance etc…) Not accessible without account credentials (username and password). Subject to persistent security scanning and checks via network-wide deployment of Sophos security software and Microsoft security features.
GSuite	GSuite is cloud based, hosted on Google servers, so subject to security features deployed and updated by Google. Please refer to Google's security and data protection policies. Cannot access data without @swale.at account credentials.
Bromcom	Database is cloud based. Please refer to Bromcom's GDPR Compliance and Privacy Statement. Not accessible without account credentials (username and password).

SIRAS	Remote desktop access for off-site usage. Two factor authentication with SIRAS credentials and AD account credentials. Not directly connected to school network.

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**

Head of Centre and 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

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 section *Table recording candidate exams-related information held* 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 every 12 months (this may include updating antivirus software, firewalls, internet browsers etc.)

6. Access to information

Current and former candidates can request access to the information/data held on them by making a subject access request to the Data Protection Officer in writing/email, with valid photo ID. All requests will be dealt with within 40 calendar days.

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.

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 consider 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

https://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

https://www.gov.uk/guidance/school-reports-on-pupil-performance-guide-for-headteachers

Publishing exam results

When considering publishing exam results, the centre will refer to the ICO (Information Commissioner's Office) Education and Families https://ico.org.uk/media/for-organisations/documents/1135/publication-of-exam-results-by-schools-dpa-guidance.pdf information on *Publication of exam results*.

7. Table recording exams-related information held and retention period

Details of retention periods, the actions taken at the end of the retention period and method of disposal.
For details of how to request access to information held, refer to the *Access to information* section of this policy.

Information type	Information description	What personal/sensitive data is/may be contained in the information	Where information is stored	How information Is protected	Retention period	Method of disposal
Access arrangements information	Any hard copy or electronic information kept by the Exams Office relating to a candidate with an access arrangement.	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 NCFE Portal MIS Lockable metal filing cabinet	Secure username and password Bromcom and ESCC software and firewalls and anti-virus	Six years	Confidential waste and deletion from computer records.
Alternative site arrangements	Any hard copy information generated on an alternative site arrangement. Notifications submitted online via CAP.	Candidate name Candidate DOB Gender	JCQ's Centre Admin Portal (CAP) Lockable metal filing cabinet	Secure username and password	To be retained until the deadline for reviews of results for the exam season has passed and any outstanding reviews or appeals or malpractice investigations are complete, whichever is later (for the exam series).	Confidential waste collection used.
Attendance registers copies	Copy of the signed attendance register for each exam. Records are kept in accordance with the requirements of JCQ's ICE, section 12, 22.6.	Candidate name	Lockable metal filing cabinet	Key stored securely by Exams Officer.	To be retained until the deadline for reviews of results for the exam season has passed and any outstanding reviews or appeals or malpractice investigations are complete, whichever is later (for the exam series).	Confidential waste collection used.

Awarding body administrative information	Hard copy publications of documents received from awarding bodies.	N/A	Exams Office	N/A	Until the current academic year update is provided.	Recycling waste.
Candidate and Centre Declarations	Hard or electronic copies of forms signed by candidates confirming the work is their own, and forms signed by teachers to confirm that candidates' work was completed under required conditions and internal standardisation has been completed if required.	Candidate name	Lockable metal filing cabinet	Key stored securely by Exams Officer.	To be retained until the deadline for reviews of results for the exam season has passed and any outstanding reviews or appeals or malpractice investigations are complete, whichever is later (for the exam series).	Confidential waste and deletion from computer records.
Candidates' scripts	Any unwanted copies of scripts returned to the centre through the Access to Scripts (ATS) service.	Candidate name	Lockable safe	Exam secure storage (only two key holders)	To be retained securely until the awarding body's earliest date for confidential disposal of unwanted scripts.	Records are kept in accordance with the requirements of JCQ's General Regulations, section 3, 3.15. Where teachers have used copies of candidates' scripts for teaching and learning purposes but no longer wish to retain them, they must ensure that the scripts are disposed of in a confidential manner. Confidential waste collection used.
Candidates' work	Non-examination assessment work returned to the centre by the awarding body at the end of the moderation period. Hard or electronic copies of candidates' work which has been sent for	Candidate name	Lockable subject storage	Key stored securely by teachers.	To be retained until the deadline for reviews of results for the exam season has passed and any outstanding reviews or appeals or malpractice investigations are complete, whichever is later (for the exam series).	Returned to candidates or disposed of using confidential waste, including deletion from computer records if necessary.

	assessment/moderation and which will not be returned to the centre.				NEA work is logged on return to the centre, subject staff notified and stored safely and securely along with work that did not form part of the moderation sample (including materials stored electronically).	
Certificate collection information	Candidate signature form and signed authorisation for third parties to collect.	Candidate name	Lockable metal filing cabinet	Key stored securely by Exams Officer.	Scanned copy stored electronically. Original retained in certificate folder, which are presented to candidates at 'Certificate Evening'. Electronic copy to be retained for 6 years after the student has left the centre. Any original certificates unable to be presented to a candidate will be retained for two years after the student has left the centre.	Confidential waste and deletion from computer records.
Certificate destruction information	A record of unclaimed certificates that have been destroyed.	Candidate name	Lockable metal filing cabinet	Key stored securely by Exams Officer.	To be retained for four years from the date of destruction.	Confidential waste collection used.
Certificates	Candidate's certificates issued by the awarding bodies.	Candidate name Candidate DOB	Lockable metal filing cabinet	Key stored securely by Exams Officer.	Two years	Confidential waste and deletion from computer records.
Confidential materials: initial point of delivery logs	Logs recording awarding body confidential exam materials received by an authorised member of staff at the initial point of delivery and the secure	N/A	Lockable metal filing cabinet	Key stored securely by Exams Officer.	To be retained until the end of the following academic year	Confidential waste collection used.

	movement of packages by an authorised member of staff to the secure room for transferal to the centre's secure storage facility.					
Confidential materials: receipt, secure movement and secure storage logs	Logs recording confidential exam materials received (including encrypted materials received via email or downloaded from an awarding body's secure extranet site), checked and placed in the secure storage facility by the Exams Officer (or other authorised member of centre staff) throughout the period the materials are confidential.	N/A	Lockable metal filing cabinet	Key stored securely by Exams Officer.	To be retained until the end of the following academic year	Confidential waste collection used.
Conflicts of Interest records	Hard copy and electronic records demonstrating the management of Conflicts of Interest.	N/A	Exams Google drive Lockable metal filing cabinet	Secure username and password. Key stored securely by Exams Officer.	To be retained until the end of the following academic year	Confidential waste and deletion from computer records.
Dispatch logs	Proof of dispatch of exam script packages to awarding body examiners covered by the DfE (Standards & Testing Agency) yellow label service.	N/A	Lockable metal filing cabinet	Key stored securely by Exams Officer.	To be retained until the end of the following academic year	Confidential waste collection used.
Entry information	Any hard copy or electronic information relating to candidates' entries.	Candidate name	Awarding body secure sites Bromcom Lockable metal filing	Secure usernames and passwords. Key stored securely by Exams Officer.	Hard copies to be retained until the end of the following academic year. Electronic information to be retained for six years.	Confidential waste and deletion from computer records, if necessary.

			cabinet			
Exam question papers (unused)	Spare, unused question papers for timetabled written exams.	N/A	Lockable safe	Exam secure storage (only two key holders)	In accordance with JCQ's GR, section 6, 6.13, copies of the question papers will not be released to centre personnel until after the awarding body's published finishing time for the exam or, in the case of a timetable variation, until all candidates within the centre have completed the exam.	Issued to relevant subject's Head of Department.
Exam room incident logs	Logs recording any incidents or irregularities in exam rooms for each exam session.	Candidate name	Lockable metal filing cabinet	Key stored securely by Exams Officer.	To be retained until the deadline for reviews of results for the exam season has passed and any outstanding reviews or appeals or malpractice investigations are complete, whichever is later (for the exam series).	Confidential waste collection used.
Exam stationary	Awarding body exam stationery provided solely for the purpose of external exams.	N/A	Exam secure storage room	Exam secure storage (only two key holders)	Unused stationary returned to secure storage room.	Out-of-date stationary destroyed - confidential waste collection used.
Examiner / Moderator reports	Hard or electronic copies of examiner/moderator reports.	N/A	Lockable metal filing cabinet	Key stored securely by Exams Officer.	To be retained for three years.	Confidential waste and deletion from computer records, if necessary.
Invigilator training records	Any hard copy or electronic information kept by the Exams Officer relating to invigilator training records.	Invigilator name	Exams Google drive Lockable metal filing cabinet	Secure username and password. Key stored securely by Exams Officer.	To be retained until the end of the following academic year.	Confidential waste and deletion from computer records, if necessary.

Invigilation arrangements	Hard and/or electronic copies of invigilation arrangements for all exams.	Invigilator name	Exams Google drive Lockable metal filing cabinet	Secure username and password. Key stored securely by Exams Officer.	To be retained until the deadline for reviews of results for the exam season has passed and any outstanding reviews or appeals or malpractice investigations are complete, whichever is later (for the exam series).	Confidential waste and deletion from computer records, if necessary.
Overnight supervision information	The JCQ Overnight Supervision form is completed online using CAP. The JCQ Overnight Supervision Declaration form is downloaded from CAP for signing by the candidate, the supervisor and the Head of Centre.	Candidate name	Lockable metal filing cabinet	Key stored securely by Exams Officer.	To be retained until the deadline for reviews of results for the exam season has passed and any outstanding reviews or appeals or malpractice investigations are complete, whichever is later (for the exam series).	Confidential waste collection used.
Post-results services: confirmation of candidate consent information	Hard copy or email record of required candidate consent for post-results service submission.	Candidate name	Lockable metal filing cabinet	Key stored securely by Exams Officer.	To be retained until the end of the following academic year.	Confidential waste and deletion from computer records, if necessary.
Post-results services: requests/outcome information	Any hard or electronic copy information relating to a post-results service request submitted to an awarding body for a candidate and outcome information from the awarding body.	Candidate name	Lockable metal filing cabinet	Key stored securely by Exams Officer.	To be retained until the end of the following academic year.	Confidential waste and deletion from computer records, if necessary.
Private candidate information	Any hard copy or electronic information relating to private (external) candidates' entries.	Candidate name Candidate contact information	Awarding body secure sites Bromcom Lockable metal filing	Secure usernames and passwords. Key stored securely by Exams Officer.	Hard copies to be retained until the end of the following academic year. Electronic information to be retained for six years.	Confidential waste and deletion from computer records, if necessary.

			cabinet			
Proof of postage – candidates' work	Proof of postage of sample of candidates' work submitted to awarding body examiners/markers/ moderators.	Candidate name Moderator's name and address	Lockable metal filing cabinet	Key stored securely by Exams Officer.	To be retained until the end of the following academic year.	Confidential waste collection used.
Resolving timetable clashes information	Any hard or electronic copy information relating to the resolution of a candidate's clash of timetabled exam papers.	Candidate name	Lockable metal filing cabinet	Key stored securely by Exams Officer.	To be retained until the end of the following academic year.	Confidential waste and deletion from computer records, if necessary.
Results information	Hard copy broadsheets and/or electronic copies of results summarising candidate final grades by subject by exam series.	Candidate name	Exams Google drive Bromcom Lockable metal filing cabinet	Secure username and password. Key stored securely by Exams Officer.	To be retained for current year plus previous 6 years.	Confidential waste and deletion from computer records, if necessary.
Seating plans	Hard copy and electronic plans showing the seating arrangements of all candidates for every exam taken, and access arrangements assigned where appropriate.	Candidate name Access arrangements	Bromcom Lockable metal filing cabinet	Secure username and password. Key stored securely by Exams Officer.	To be retained until the deadline for reviews of results for the exam season has passed and any outstanding reviews or appeals or malpractice investigations are complete, whichever is later (for the exam series).	Confidential waste and deletion from computer records, if necessary.
Special consideration information	Any hard copy information relating to a special consideration application which has been submitted to an awarding body for a candidate, and signed evidence produced by a senior leader in support of the application (where necessary). The special	Candidate name Personal details of application	Awarding body secure sites Lockable metal filing cabinet	Secure usernames and passwords. Key stored securely by Exams Officer.	To be retained until the end of the following academic year.	Confidential waste and deletion from computer records, if necessary.

	consideration form is completed online using the awarding body's secure site.					
Suspected malpractice reports/outcomes	Any hard or electronic copy information relating to a suspected or actual malpractice investigation, including any reports submitted to an awarding body and outcome information from the awarding body.	Candidate name Personal details of investigation	Exams Google drive Exam secure storage room	Secure username and password Exam secure storage (only two key holders)	To be passed to Head of Centre and in line with the centre's malpractice policy. To be retained until the end of the following academic year.	Confidential waste and deletion from computer records, if necessary.
Very late arrival reports/outcomes	Any hard or electronic copy information relating to a candidate arriving very late to an exam. Reports submitted online via CAP.	Candidate name	Lockable metal filing cabinet	Key stored securely by Exams Officer.	To be retained until the end of the following academic year.	Confidential waste and deletion from computer records, if necessary.

This policy has been reviewed and authorised by:

_____

Rachel Henocq
Headteacher / Head of Centre