Heathfield
COMMUNITY SCHOOL

General Data Protection Regulation Policy (Exams)

Contacts and Review Information

Data Protection Officer	dposchools@somerset.gov.uk
School Data Protection Lead	Stuart Walker
The policy was approved by Governors / Trustees on:	_____
Signature of Chair of Governors / Trustees:	_____
The next review date is:	_____

Amendments to the previously approved policy are highlighted.

Contents

Key Staff

Role	Names
Head of Centre	Peter Hoare
Exams Officer	Lionel Crow
Data Manager	Jackie Baddoo
IT Support	Alan Higginson
Data Protection Officer	Stuart Walker

Purpose of the Policy

This policy details how Heathfield Community 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).

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 and 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 officer 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
- Department for Education
- Local Authority
- The press (no names will be released)

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

- Hard copy
- E-mail

- Secure extranet sites – e.g. eAQA; OCR Interchange, Pearson, Edexcel Online and WJEC Secure Services
- Capita SIMS
- 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 exams results/post-results/certificate information.

Section 2 – Informing Candidates of the Information Held

Heathfield Community School ensures that candidates are fully aware of the information and data held.

All candidates are:

- informed via a Student Privacy Notice displayed on the school website
- given access to this policy via written request

Candidates are made aware of the above at the start of their course of study leading to an externally accredited qualification and in the examination guidance for parents and students booklet.

At this point, Heathfield Community School also brings to the attention of candidates the annually updated JCQ document *Information for candidates – Privacy Notice* which explains how JCQ awarding bodies process their personal data in accordance with the DPA 2018 and GDPR

Section 3 – Hardware and Software

The table below confirms how IT hardware, software, and access to online systems are protected in line with DPA & GDPR requirements.

Hardware	Protection measures
Desktop computer	Administrator access restricted to IT Support staff; PC protected by Microsoft Endpoint & Defender; monthly security updates automatically deployed; users access profiles created for role specific requirements. Fully networked PC. Computers checked at least once a year for faults (IT Support check for errors, general check for speed and usability) Anti-virus is updated centrally. All Internet browsing takes place on a controlled connection, based on rules set for education.
Laptop computer	As above
File Server(s)	All stored on a secure area on Microsoft network server(s). Systems have restricted administrator access, full back-up regime and user access to data is controlled. External access to networks by default all IT equipment is protected by a combination of layers of security. Passwords are valid for 90 days then are compulsory changed.
Data Transfer – WIFI	All systems transferring data via corporate WIFI are encrypted to WPA2 Enterprise level.

Software/online system	Protection measure(s)
MIS (Capita SIMS)	Protected usernames and passwords; centre administrator has to approve the creation of new user accounts and determine access rights

Internet browser(s)	Student web filter; regularly updated firewall and anti-virus software
Awarding body secure extranet sites • **eAQA;** • **OCR Interchange;** • **Pearson Edexcel Online;** • **WJEC secure access;** • **RSL;** • **UAL.**	• Access controlled by username and password; • Accounts have specified access rights; • Centre administrator has to approve the creation of new user accounts and determine access rights.
A2C	Installed only on centre administrator's computer

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 unauthorized use
- Equipment failure
- Human error
- Unforeseen circumstances such as a fire or flood
- Hacking attack
- 'Blagging' offences where information is obtained by deceiving the organization who holds it

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

1. Containment and recovery

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 recognize when someone tries to use stolen data to access accounts
- Which authorities, if relevant, need to be informed

2. Assessment of on-going 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 yearly.

The table below details the type of 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
- Microsoft Endpoint updated daily
- Microsoft Windows updates and patches as released

Section 6 – Data Retention Periods

The School will follow the advice from the IRMS using their Records Management Toolkit for schools in respect of retention periods, the actions taken at the end of the retention period, and the methods of disposal.

Section 7 – Access to Information

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

5. Third Party Access

Permission should be obtained before requesting personal information on another individual from a third-party organization.

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 in 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.

6. 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

7. Publishing exam results

When considering publishing exam results, the centre will make reference to the ICO (Information Commissioner's Office) Education and Families https://ico.org.uk/for-organisations/education/ information on Publishing exam results.

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	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 Learning Support Department	Secure name and password In a locked filing cabinet	After the deadline for EARs
Attendance registers copies	Candidate name Candidate number Candidate tier information (where applicable)	The exams office	In secure area solely assigned to exams	After the deadline for EARs
Candidates' scripts	Candidate name Candidate number Candidate tier information Candidate assessment data	Classrooms Staff learning rooms The exams office	Lockable cabinets within staff learning rooms and classrooms Students are forbidden from entering staff learning rooms The exams office is always locked	n/a
Candidates' work	Candidate name Candidate number Candidate tier information Candidate assessment data	Classrooms Staff learning rooms The exams office	Lockable cabinets within staff learning rooms and classrooms Students are forbidden from entering staff learning rooms The exams office is always locked	After the deadline for EARs
Certificates	Candidate name	The exams office	The exam office is always locked	One year after

Information Type	What personal/sensitive data is/may be contained in the information	Where information is stored	How information is protected	Retention period
	Candidate number Candidate DoB Unique Candidate Identifier (UCI) Qualification grades			certificate evening
Certificate destruction information	Candidate name Candidate number Unique Candidate Identifier	The exams office	The exams office is always locked	
Certificate issue information	Candidate name	The exams office	The exams office is always locked	
Entry information	Candidate name Candidate number Candidate tier information (where applicable)	MIS Exams Officer's computer The exams office	Secure user name and password In secure area solely assigned to exams	
Exam room incident logs	Candidate name Candidate number Details of incident involving candidate(s)	The main exam venue The exams office	In possession of lead invigilator The exams office is always locked	After the deadline for EARs and/or appeals have been exhausted
Invigilator and facilitator training records	Invigilator name Attendance	The exams office	The exams office is always locked	After the deadline for EARs and/or appeals have been exhausted
Overnight supervision information	Candidate name Candidate number Details of overnight supervision arrangements Candidate address Candidate contact details	The exams office	The exams office is always locked	After the deadline for EARs and/or appeals have been exhausted
Post-results services: confirmation of candidate consent	Candidate name Candidate number	The exams office	The exams office is always locked	After the deadline for EARs and/or appeals have been

Information Type	What personal/sensitive data is/may be contained in the information	Where information is stored	How information is protected	Retention period
information				exhausted
Post-results services: scripts provided by ATS service	Candidate name Candidate number Qualification grades and marks Candidate answers to questions	IT network Awarding body secure extranet site Staff learning rooms Classrooms The exams office	Secure user name and password Lockable cabinets within staff learning rooms and classrooms The exams office is always locked	After the deadline for EARs and/or appeals have been exhausted
Post-results services: tracking logs	Candidate name Candidate number	Exams Officer's computer The exams office	Secure user name and password The exams office is always locked	After the deadline for EARs and/or appeals have been exhausted
Private candidate information	Candidate name Candidate number Candidate UCI Candidate ULN Candidate DoB Gender Candidate timetable	MIS Exams Officer's computer Awarding body secure extranet site The exams office	Secure user name and password The exams office is always locked	After the deadline for EARs and/or appeals have been exhausted
Resolving clashes information	Candidate name Candidate number Candidate UCI Candidate timetable	MIS Exams Officer's computer The exams office	Secure user name and password The exams office is always locked	After the deadline for EARs and/or appeals have been exhausted
Results information	Candidate name Candidate number Candidate UCI Candidate ULN Candidate DoB Qualification grades	MIS Exams Officer's computer The exams office Awarding body secure extranet site Teacher reports	Secure user name and password In secure area solely assigned to exams Lockable cabinets within staff learning rooms and classrooms	
Seating Plans	Candidate name Candidate number	Exams Officer's computer	Secure user name and password The exams office is always	After the deadline for EARs and/or

Information Type	What personal/sensitive data is/may be contained in the information	Where information is stored	How information is protected	Retention period
	Candidate UCI	The exams office Exams venues	locked	appeals have been exhausted
Special consideration information	Candidate name Candidate number Candidate UCI Candidate DoB Medical details (if applicable) Safeguarding information (if applicable)	Awarding body secure extranet site The exams office Pastoral leader	Secure user name and password The exams office is always locked	After the deadline for EARs and/or appeals have been exhausted
Suspected malpractice reports/outcomes	Candidate name Candidate number Candidate UCI Qualification codes Personal details as pertaining to the incident Evidence	Exams Officer's computer The exams office Awarding body malpractice dept.	Secure user name and password The exams office is always locked Email correspondence with awarding body	
Transfer of credit information	Candidate name Candidate number Candidate UCI Candidate ULN Entry codes Tier information (where applicable)	The exams office Awarding body extranet Destination school	Secure user name and password The exams office is always locked Email correspondence with destination school	
Transferred candidate information	Candidate name Candidate number Candidate UCI Candidate ULN Entry codes Tier information (where applicable)	The exams office Awarding body extranet Previous school	Secure user name and password The exams office is always locked Email correspondence with previous school	
Very late arrival reports/outcomes	Candidate name Candidate number Entry codes	The exams office Awarding body	Secure user name and password Email correspondence with awarding body The exams office is always locked	