

Data Protection Policy (Exams)

2020/21

This policy is reviewed annually to ensure compliance with current regulations

Approved/reviewed by	
Mrs M Walker	
Date of next review	Sept 2021

Key staff involved in the policy

Role	Name(s)
Head of centre	Mrs M Walker
Exams officer	Mrs A Ashton
Senior leader(s)	Mr S Blower
IT manager	Mr J Kumar
Data manager	Mr A Shelton

Purpose of the policy

This policy details Colton Hills 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).

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)
- 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) – [insert as appropriate to your centre e.g. eAQA; OCR Interchange; Pearson Edexcel Online; WJEC Secure Website; City & Guilds Walled Garden; etc.]
- [insert any other methods as appropriate to your centre e.g. a Management Information System (MIS) provided by [insert MIS provider detail (e.g. Capita 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

Colton Hills Community 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 centre website, written request, etc.

Candidates are made aware of the above 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
Desktop computer; Laptop/tablet; etc.	Hardware is checked; by who; what is checked (hard drive scans etc.); antivirus protection up to date; etc.	N/A
Room S6 HP 8300	July 2013 Checked by JKU & DSU Antivirus Used Windows Security updated via Intune - daily	No Warranty
Room S45, HP ProDesk 400 G6 SFF Desktop PC - Intel Core i5-9500 (9MB Cache, 3GHz), 8GB DDR4-SDRAM, 256GB SSD, Intel UHD Graphics 630, LAN, Windows 10 64-bit	July 2019 Checked by JKU & DSU Antivirus Used Windows Security updated via Intune – daily	Warranty 5yrs
HP Room S46 S48 HP ProDesk 400 G6 SFF Desktop PC - Intel Core i5-9500 (9MB Cache, 3GHz), 8GB DDR4-SDRAM, 256GB SSD, Intel UHD Graphics 630, LAN, Windows 10 64-bit	July 2020 Checked by JKU & DSU Antivirus Used Windows Security updated via Intune – daily	Warranty 5yrs
Laptops HP Pro 450, g5	July 2018 Checked by JKU & DSU Antivirus Used Windows Security updated via Intune – daily	Warranty 5yrs

Software/online system	Protection measure(s)
Students taking exams have their own personal logins and password.	The area is secured with NTFS permissions so that students cannot access other candidates' area. The exam material is stored on our secured network and also backed up on an external storage device.
MIS; Intranet; Internet browser(s); Awarding body secure extranet site(s); A2C; etc.	Protected usernames and passwords; rules for password setting (use of a mix of upper/lower cases 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; etc.

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

Mr Gerald O Hara 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

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 daily 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 see Exams archiving policy which is available/accessible from exams office and 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 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 Gerald O Hara Data Protection Officer in writing/email and how 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.

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

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 [insert your centre's process for sharing data with a third-party e.g. 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

When considering publishing exam results, Colton Hills School will make reference to the ICO (Information Commissioner's Office) Schools, universities and colleges information <https://ico.org.uk/your-data-matters/schools/> on Publishing exam results.

(Publishing examination results is a common and accepted practice. Many students enjoy seeing their name in print, particularly in the local press and the GDPR does not stop this happening. However, under the GDPR schools have to act fairly when publishing results, and where people have concerns about their or their child's information being published, schools must take those concerns seriously.)

Schools should make sure that all pupils and their parents or guardians are aware as early as possible whether examinations results will be made public and how this will be done. Schools should also explain how the information will be published. For example, if results will be listed alphabetically, or in grade order.

In general, because a school has a legitimate reason for publishing examination results, pupils or their parents or guardians do not need to give their consent to publication. However, if you have a specific concern about publication of your results, you have the right to object. Schools should consider objections from pupils and parents before making a decision to publish. A school would need to have a good reason to reject someone's objection to publication of their exam results.)

OR

Colton Hills School 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
- 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 [insert centre name] will have a legitimate reason for publishing examination results, consent is not required from students or their parents or guardians for publication. However, if a student or their parents or guardians have a specific concern about publication of their results, they have the right to object. This objection must be made in writing to [insert name/role of individual], 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.

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	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		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 office (SENCo)	
Alternative site arrangements		Candidate name Examination Number	Exams Office	Locked in cabinet	
Attendance registers copies		Candidate name Examination Number	Exams Office	Locked in cabinet	
Candidates' scripts		Candidate name Examination Number	Exams Office	Locked in secure store room	
Candidates' work		Candidate name Examination Number	Exams Office	Locked in cabinet	

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
Centre consortium arrangements for centre assessed work		Candidate name Examination Number	Exams Office	Locked in cabinet	
Certificates		Candidate name Examination Number Candidate Results	Exams Office	Locked in cabinet	
Certificate destruction information		Candidate name Examination Number Candidate Results	Exams Office	Secure user name and password	
Certificate issue information		Candidate name Examination Number	Exams Office	Locked in cabinet	
Conflicts of Interest records		Staff Name	Exams Office	Locked in cabinet	
Entry information		Candidate name Examination Number	Exams Office	Locked in cabinet	
Exam room incident logs		Candidate name Examination Number	Exams Office	Locked in cabinet	
Invigilator and facilitator training records		Invigilators Name and signature	Exams Office	Locked in cabinet	

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
Overnight supervision information		Candidate name Examination Number	Exams Office	Locked in cabinet	
Post-results services: confirmation of candidate consent information		Candidate name Examination Number	Exams Office	Locked in cabinet	
Post-results services: requests/outcome information		Candidate name Examination Number	Exams Office	Locked in cabinet	
Post-results services: scripts provided by ATS service		Candidate name Examination Number	Exams Office	Locked in cabinet	
Post-results services: tracking logs		Candidate name Examination Number	Exams Office	Locked in cabinet	
Private candidate information		Candidate name Examination Number	Exams Office	Locked in cabinet	
Resolving timetable clashes information			Exams Office	Locked in cabinet	
Results information		Candidate name Examination Number Candidate Results	Exams Office	Secure user name and password	

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
Seating plans		Candidate name Examination Number	Exams Office	Locked in cabinet	
Special consideration information		Candidate name Examination Number Doctors notes and evidence	Exams Office	Locked in cabinet	
Suspected malpractice reports/outcomes		Candidate name Examination Number	Exams Office	Locked in cabinet	
Transferred candidate arrangements		Candidate name Examination Number	Exams Office	Locked in cabinet	
Very late arrival reports/outcomes		Candidate name Examination Number	Exams Office	Locked in cabinet	