**JOHN SPENDLUFFE**

**TECHNOLOGY COLLEGE**



**Examinations**

**GDPR Policy**

**2023 -2024**

# Key staff involved in the General Data Protection Regulation policy

|  |  |
| --- | --- |
| **Role**  | **Name(s)**  |
| Head of centre  | **Mr Simon Curtis**  |
| Exams officer | **Mrs J Bishell** |
| Exams officer line manager (Senior Leader) | **Miss R Norton** |
| Data Protection Officer | **Mr J Treasure**  |
| Network manager  | **Mr C Knight**  |
| Data manager  | **Mr J Bentley**  |

# Purpose of the policy

This policy details how John Spendluffe Technology College in relation to exams management and administration, ensures compliance with the regulations as set out by the Data Protection Act (DPA) and 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 these *General Regulations* 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 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

To ensure that the centre meets the requirements of the DPA 2018 and UK 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), (EO) 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

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

* hard copy
* email
* Secure extranet site(s) – eAQA; Centre Services (AQA), OCR Interchange; Pearson Edexcel Online; WJEC Secure services.
* Management Information System (MIS) provided by Serco Bromcom, SMiD, 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.

# Section 2 – Informing candidates of the information held

JSTC ensures that candidates are fully aware of the information and data held.

All candidates are:

 informed via Privacy Notice on Admission to school to parents and candidates. Information also outlined in GCSE Handbook.

 given access to this policy via JSTC website and hard copy.

Candidates are made aware of the above on admission and at the at the start of a course leading to a vocational qualification, or, 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 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  |
| MS Windows Desktop Computers  | Various  | Various  |
| MS Windows Laptop Computers  | Various  | Various  |
| 2 x VMware ESXi Hypervisor Hosts  | Various  | Various  |
| 1 x SAN (data storage medium)  | Various  | Various  |
| Multiple MS Windows Servers (various versions) operating on virtually hardware and dedicated hardware.  | Various  | Various  |

|  |  |
| --- | --- |
| Software/online system  | Protection measure(s)  |
| Bromcom (MIS – back end)  | Access to Bromcom Admin is restricted by multiple layers. Layer 1: Access to the JSTC network by the means of a username and minimum 8 character password, requiring password complexity routines and password history restrictions. Layer 2: Only authorised staff users have access to the Bromcom Admin back end program. Layer 3: Only authorised Bromcom Admin Users are provided with a separate username and password to access the system Layer 4: Specific modules (areas) of the Bromcom Admin are restricted to specific users.  |
| A2C Data transfer system within Bromcom | Data is encrypted between AB’s and Bromcom. Access is restricted to relevant roles being enabled i.e. EO and LM to EO, HoC & Data Manager. |
| Desktops and Servers Antivirus Protection  | Desktop and Server Antivirus protection is installed and updated at a minimum of once every hour. Automatic reporting of an outbreak is enabled. Frequent checking of  |
|  | any issues is performed via a central console.  |
| Awarding Body’s Extranet website  | EO creates accounts and passwords initially. Staff then have to change the password on first logging in. EO deletes accounts of staff members no longer at JSTC.  |

# 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 hold it
* Cyber-attacks involving ransomware infections

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

## 1. Containment and recovery

Mr J Treasure, 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

# 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.

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 every 6 months (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 will be contained in the centre’s Exams Archiving Policy. Available on request from Mr J Treasure, Data Protection Officer.

# 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 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 exam questions.

**Requesting exam information**

Requests for exam information can be made by current and former candidates and request access to the information/data held on them by making a **subject access request** to Mr J Treasure, Data Protection Officer requests can be made electronically or in writing ID will be needed to confirm if a former candidate is unknown to current staff. All requests will be dealt with within 40 calendar days.

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.

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 by Deputy Head, LM to Exams and DPO 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 exam results have been published, 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 only be shared with a third party as outlined in JSTC’s Privacy Notice and only to those listed within this notice. The Privacy Notice is available on the school website or can be requested from the school. Or unless a request is accompanied with permission from the candidate and appropriate evidence (where relevant), to verify the ID of both parties, will data be shared with a third party.

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.

# 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 Lockable metal filing cabinet    | Limited access to the folder on Department Drive SEN   | 1 year  |
| Attendance registers copies  | Candidate name Candidate Number  | Hard Copy lockable filing cabinet  | Restricted access – 3 key holders  | Until RORs deadline for outcomes  |
| Candidates’ work  | Candidate name Candidate Number  | Lockable filing cabinet | Restricted Access by departments  | Until RORs deadline for outcomes  |
| Certificates  | Candidate name Candidate Number Exams taken | Lockable filing cabinet  | Restricted access  | 3 years from Certificate issue in the November of the year of results release  |
| Certificate destruction information  | Candidate name Candidate Number Exams taken    | Exam folder in Excel  | Restricted access on Admin drive  | 9 years  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Information type**  | **What personal/sensitive data is/may be contained in the information**  | **Where information is stored**  | **How information is protected**  | **Retention period**  |
| Certificate issue information  | Candidate name Candidate Number Candidate signature   | Lockable cabinet  | Restricted access  | 9 years  |
| Conflicts of interest information  | Name   | Microsoft Form  | Restricted access  | 2 years  |
| Entry information  | Candidate name Candidate Number Candidate ULN Candidate DOB Candidate UCI   |  MIS | Secure Password EDI via A2C secure data exchange  | 9 years  |
| Exam room incident logs  | Candidate name Candidate Number   | Lockable storage unit  | Restricted Access in exams office  | Until RORs deadline for outcomes  |
| Overnight supervision information  | N/A  | N/A  | N/A  | N/A  |
| Post-results services: confirmation of candidate consent information  | Candidate name Candidate Number Exam information Candidate Signature  | Lockable filing cabinet  | Restricted Access  | 6 months  |
| Post-results services: requests/outcome information  | Candidate name Candidate Number Exam information  | Awarding Body Secure Websites  | Secure password – EO only  |   |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Information type**  | **What personal/sensitive data is/may be contained in the information**  | **Where information is stored**  | **How information is protected**  | **Retention period**  |
|  |   |  |  |  |
| Post-results services: scripts provided by ATS service  | Candidate name Candidate Number Exam information   | Lockable Filing cabinet   | Limited Access by secure password EO only  | 1 Year  |
| Post-results services: tracking logs  | Candidate name Candidate Number Exam information   | Exam folder in Excel  | Restricted Access on Admin Drive  | 3 Years  |
| Private candidate information  | Candidate name Candidate Number Exam information   | MIS  | Restricted Access Password  | 9 years  |
| Resolving clashes information  | Candidate name Candidate Number Exam information   | MIS  | Restricted Access Password  | 1 year  |
| Results information  | Candidate name Candidate Number Candidate ULN Candidate DOB Candidate UCI   | MIS Data Analysis Programme   | Restricted Access Password  | 9 years  |
| **Information type**  | **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 Candidate Number Access Arrangement information  | Exam Folder in Excel, Hard copies lockable filing cabinet  | Restricted access on Admin Drive Restricted key access 3 key holders  | 1 Year  |
| Special consideration information  | Candidate name Candidate Number Exam information  | Awarding Bodies Secure Websites  | Password protected – EO only  | Until RORs deadline for outcomes  |
| Suspected malpractice reports/outcomes  | Candidate name Candidate Number Exam information  | Awarding Bodies Secure Websites  | Password protected – EO only  | Until RORs deadline for outcomes  |
| Transfer of credit information  | N/A  |   |   |   |
| Transferred candidate information  | N/A  |   |   |   |
| Very late arrival reports/outcomes  | Candidate name Candidate Number Exam information  | Awarding Bodies Secure Websites  | Password protected – EO only  | Until RORs deadline for outcomes  |