Stockport School

Data Protection Policy

Purpose of the plan

This policy details how Stockport 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 Stockport School 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 to hold exams-related information on candidates taking external examinations.

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

- Awarding bodies
- Joint Council for Qualifications (JCQ)
- any other organisations as relevant to Stockport School e.g. Department for Education; Local Authority;

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

- hard copy
- email
- secure extranet site(s) – e-AQA; OCR Interchange; Pearson Edexcel Online; WJEC Secure Website; NCFE secure portal or any other exam boards that we are using at the time that the student is sitting their examinations
- our SIMS Management Information System (MIS sending/receiving information via electronic data interchange (EDI) using A2C to send to and receive 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

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

All candidates are:

- given access to this policy via centre website or if they request it in writing

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 via their Exam Handbook which is given out in Year 11.

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.

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**

The Headteacher or Assistant headteacher 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.

Once all investigations have taken place the Local Authority Data Protection Officer will be informed

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

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

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 Exams archiving policy which is available/accessible from the school website.

Exam Certificates that are not collected by the former student will be kept for a period of 10 years (until the students reach the age of 25 years) and will form part of the Student Records.

Access to information

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 the Exams Officer or Assistant Headteacher in charge of exams in writing or by email. An administration fee of £10.00 is payable for any Statement of Results that is produced. The student/or former students must collect the information themselves or can authorise someone to collect it on their behalf in writing and the person collecting the Statement must bring with them photocopy ID for themselves.

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 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, a letter of authority from the candidate is needed before any results can be shared.

Sharing information with parents

No exam results will be shared with parents without the written authority from the candidate. Any parent wanting the results of the student must apply to the Headteacher in writing with requests considered on a case by case basis. The Headteacher 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.

Publishing exam results

At present the exam results are not published in any newspaper etc but if it was to be considered then the candidates would be informed.

Review:

This Plan will be reviewed on an annual basis in conjunction with the Examinations Policy

Last Review: September 2020

Next Review: September 2021