Exam Data Protection Policy

Responsibility:	G.Alvarado
Version Date:	December 2021
Review Date:	September 2022

This policy details how Lister 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 UK General Data Protection Regulation (GDPR). This policy should also be read with the Lister Community School Data Protection Policy.

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. (JCQ General Regulations for Approved Centres (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.

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)
- 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) –e.g. eAQA; OCR Interchange; Pearson Edexcel Online; WJEC Secure Website;
- SIMS, A2C, Go4Schools

Informing candidates of the information held

The candidates are given the JCQ Information for Candidates 'Information About You and How We Use It' notice to inform them of how the examining body uses personal data.

Candidates eligible for access arrangements are also required to provide their consent by signing the GDPR compliant JCQ candidate personal data consent form before access arrangements

approval applications can be processed online. This form will be kept on file.

Dealing with data breaches

Although data is handled in line with DPA/UK 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
- information obtained by deception

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

Containment and recovery

Safeguarding Lead/Data Protection Officer 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.
- 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 need to be informed
- 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?
- identify the individual(s)
- 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

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 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
- 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

All candidates' exam-related information will be handled in line with DPA/UK GDPR guidelines.

Access to information

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

Exam information can be requested through the exams office email that is handled by the Exams Officer and Data Protection Officer.

The candidate will have to provide a written request for exams information, confirming details. Photographic ID will need to be provided if they are collecting documents such as Statement of Results or certificates.

Sharing information with parents - Results

Requests for examination results from an individual with parental responsibility will be met by the school in line with DfE guidance. This included both 'resident' and 'non-resident' parents. Individuals with parental responsibility will need to provide appropriate photographic ID.

Third party access

Candidates' personal data will not be shared with a third party, such as the local media, unless a request is accompanied with written permission from the candidate and appropriate evidence (where relevant), to verify the identification 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. The centre's Data Protection Officer will confirm the status of these agreements and approve/reject any requests.