General Data Protection Regulation policy (exams)

(May 2018)

This policy is annually reviewed to ensure compliance with current regulations

Key staff involved in the General Data Protection Regulation policy

Headteacher
Exams Officer
Exams Officer Line Manager (Senior Leader)
Data Protection Officer
IT Manager

Purpose of the policy

This policy details how Lawn Manor Academy, 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).

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 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
- Department for Education
- Local Authority
- Multi Academy Trust
- Consortium
- Press
- NCFE
- Trinity College
- TLM
- GL Assessment
- Colleges
- Schools/Academies
- Employers

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

- hard copy
- email
- eAQA
- OCR Interchange
- Pearson Edexcel Online
- WJEC Secure services
- Management Information System (MIS) provided by 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 exam results/post-results/certificate information.

Section 2 – Informing candidates of the information held

Lawn Manor Academy ensures that candidates are fully aware of the information and data held.

All candidates are:

- informed via centre newsletter, electronic communication
- given access to this policy via centre website, written request

Section 3 – Hardware and software

Microsoft devices (computers and laptops) are used by students for examination purposes.

These are subject to a rolling purchase programme and so dates of purchase vary. The warranties of all devices used for exams have expired, however a stock of spare devices is held, and hardware failures can be fixed expeditiously.

Software installed and online systems used on Microsoft devices used for exams may include all of or some of the following:

- Locally installed school software (for example Office)
- Locally installed faculty software (for example Python, Mira)
- Internet browsers (for example Internet Explorer, Chrome)
- Cloud based student software (for example Accelerated Reader, Hegarty Maths)
- Awarding body secure extranet sites (for example GL Assessment)

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

1	Anti-virus software is installed on all networked Microsoft devices. The Management Console is periodically updated. The server checks the internet every hour for updated virus definitions, and new definitions are downloaded to individual devices every 2 hours. Periodic checks are made that this process is working correctly.
2	All incoming network traffic to the school comes through its Internet Service Provider, and is protected by an internal Firewall. Traffic from the outside world to the Internet Service Provider is also protected by their Firewall.
3	All incoming network traffic to the school is protected by its Internet Service Provider's filtering software. There is scope for the school to tailor some filtered traffic to meet its specific requirements.
4	All incoming emails to the school come through its Internet Service Provider's email protection filtering software.
5	Operational measures including internal policies exist to maintain site wide data access and security awareness, consistency and compliance.
6	Access to all devices and data is restricted to that which is necessary, using methods including network policies, user profiling, permissions and individual usernames and passwords.
7	A rolling device re-imaging programme exists to ensure software version and software update control, device consistency and storage management.
8	Student and staff devices are distinct.
9	Data virtualisation is utilised to provide optimum resilience and disaster recovery.
10	Nightly data backups (to another building) that are checked the following morning, termly backups to external drives (held in a safe) and annual backups (held in a safe) protect historic data.
11	All new user network and email accounts are created by the Network Manager, and any non-staff account access is requested and detailed in writing by a member of the Senior Leadership Team or a Lead Professional.
12	Real-time access to devices by students can be monitored remotely via classroom management software.

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**

The 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 as appropriate.

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

Section 7 – Access to information

Current and former candidates can request access to the information/data held on them by making a **subject access request** to the Exam Office in writing and will be required to identify themselves through two forms of ID if they are not known to the exams officer. All requests will be dealt with within 40 calendar days.

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, 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/Year Leader will confirm the status of these agreements and approve/reject any requests.