General Data Protection Regulation Policy (exams)

2017/18

This policy is annually reviewed to ensure compliance with current regulations

Approved/reviewed by	
Date of next review	

Key staff involved in the General Data Protection Regulation policy

Role	Name(s)
Head of centre	**Mrs Vicki Setters- The Short Stay School for Norfolk** **Mrs Sandra Govender-The Pinetree School**
Exams officer	**Mrs Nikki Button (Locksley), Mrs Celeste White (Douglas Bader) Ms Melissa Brennock (Rosebery) Ms Julie Cox (Pinetree)**
Exams officer line manager (Senior Leader)	**Mrs Vicki Setters**
Data Protection Officer	**TBC**
IT manager	**Mr I Wooltorton**
Data manager	**Mrs Lesley Moore**

Purpose of the policy

This policy details how The Engage Trust (The Short Stay School and Pinetree), 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
- The Engage Trust, Department for Education, Norfolk County Council

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

- hard copy
- email
- secure extranet site(s) –. eAQA; OCR Interchange; Pearson Edexcel Online; WJEC Secure services; VTCT, NCFE, Arts Award, OCR.]

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

The Engage trust ensures that candidates are fully aware of the information and data held.

All candidates are:

- informed via JCQ data privacy notice
- given access to this policy via the centre website, written request.
- Candidates are made aware of the above when entries are made for examinations.

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	Sept 2016. Fully networked PC. Protected by Avast Software (Anti-Virus) – automatically updates and scans.	N/A
	Firewall is provided by Fortinet Fortigate installed with domain controller, through which all network data traffic passes and is filtered.	

Software/online system	Protection measure(s)
Candidate information stored on a secure drive on network	Access is limited and has to be agreed by Exams Officer.
SIMS (MIS)	Candidate numbers are stores here – protected by Hosted Sims access protocols.
Exam Board Secure Log-ins	All secure sites and are password protected. Access is limited and controlled by the Exams Officer.

Online Testing – Pearson 'POP' software	Bespoke designed online testing platform. Controlled access, secure log in.

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.

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 as and when they are released - software and operating systems set to update automatically.

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 policy regarding retention and is available from the school office.

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 Data Protection Officer in writing/email and

ID will be required if the former candidate is not known to current staff. 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 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	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 Fire proof Metal safe	Secure user name and password In secure area solely assigned to exams	
Attendance registers copies		Candidate Name DOB	Fire proof Metal safe		
Candidates' work					
Certificates		Candidates Name Date of Birth	Fire proof metal safe		2 years
Entry information		Candidate Name, DOB, Gender,	Awarding bodies secure sites Secure network drive internally with restricted access		
Exam room incident logs		Candidate Name	Fire proof metal safe		2 years

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
Results information	**Downloaded results information from the awarding bodies.**	Candidate Name DOB Gender	Secure area on school network.	Access is limited via network protocols to exams staff and Senior Leaders	5 years
Seating plans		Candidate Name	Secure area on school network.	Access is limited via network protocols to exams staff and Senior Leaders	5 Years
Special consideration information		Candidate Name DOB Gender Medical Information/Doctors Letter	Secure Metal safe	Restricted Access	5 years
Suspected malpractice reports/outcomes		Candidate Name DOB	Secure Metal Safe	Restricted Access	5 years