WOODLANDS SCHOOL
PURSUE EXCELLENCE & SEIZE OPPORTUNITIES

General Data Protection Regulation Policy (Exams) 2018/19

Amended: October 2018

Approved by Governors: December 2018

Review date: October 2019

Reviewing Panel: Standards, staffing and curriculum (SSC)

Key staff involved in the General Data Protection Regulation policy

Role	Name(s)
Head of centre	**Simon Cox**
Exams officer	**Honor Dignan-Roth**
Exams officer line manager (Senior Leader)	**Jessica Reynolds**
Data Protection Officer	**Donald Wykes**
IT manager	**Matt Connelly**
Data manager	**Honor Dignan-Roth**

Purpose of the policy

This policy details how Woodlands 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).

Pupils 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 2018 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; PiXL; overall school performance shared with local press.

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; City & Guilds Walled Garden; NCFE; VTCT; IFS
- Capita SIMS; MossPAM; SMID; EDI using A2C (https://www.jcq.org.uk/about-a2c)

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

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

All candidates are:

- informed via candidate handbook, private candidate information letter
- given access to this policy via Woodlands School website

Candidates are made aware of the above prior to exam entries being made, upon receipt of private candidate information letter.

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 GDPR.

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
CC4 Network - Desktop computer	Purchase Date: 28/11/2013 Antivirus scan (daily, automatic) Antivirus updated (Every 4 hours, automatic) Software restriction policies (instant, automatic).	N/A
CC4 Network - Laptop	28/11/2013 Antivirus scan (daily, automatic) Antivirus updated (Every 4 hours, automatic) Software restriction policies (instant, automatic).	N/A
Admin Network – Desktop computer	[10/01/2014] Antivirus (Sophos) daily scans Antivirus (Sophos) daily updates (every 5 hours) Hardware checked regularly (4 weeks)	N/A

Software/online system	Protection measure(s)
RM CC4 Network: Server Operating System - Windows 2008 R2	Servers are kept in a secure location restricted to specific staff. Logins for the servers are protected by passwords.
Admin Network: Server Operating System – Windows 2008 R2	Server is kept in a secure location restricted to specific staff. Login for the server is protected by a password.
MIS (SIMS)	Access level determined by permission level (as set by the Head). Usernames are protected by passwords.
A2C	Unique key codes given by exam board to secure login Loaded onto Exam Officers PC which is protected by personal username and password
Awarding body extranets: Pearson AQA OCR NCFE	Exam officer managers account permissions for the school Unique usernames and personal passwords
Online Analysis tools – PAM & SMID	Systems are set for an embargo day as per MIS Personal accounts set up with secure username and password

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

Donald Wykes (Data Protection Officer), Honor Dignan-Roth (Exams Officer) & Simon Cox (Head of Centre) 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 annually (at each year group consultation event).

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 day –
    - Antivirus (updated every 4 hours, scanned daily)
    - Windows updates (as provided by Microsoft)

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 on the Woodlands School website, a hard copy is also kept in the exams 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 Simon Cox (Head of Centre) in writing, ID will need to be produced if a former candidate is unknown to current staff writing – as per the Statutory Request for Information policy (available on the Woodlands School website). 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. Woodlands School's process for sharing data with a third-party can be found in the Statutory Request for Information policy which is available on the Woodlands School website.

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.

Sharing information with parents

The centre 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:

- **Understanding and dealing with issues relating to parental responsibility**
www.gov.uk/government/publications/dealing-with-issues-relating-to-parental-responsibility/understanding-and-dealing-with-issues-relating-to-parental-responsibility
- **School reports on pupil performance**
www.gov.uk/guidance/school-reports-on-pupil-performance-guide-for-headteachers

Publishing exam results

When considering publishing exam results, the centre will make reference to the ICO (Information Commissioner's Office) **Education and Families** https://ico.org.uk/for-organisations/education/ information on *Publishing exam results*.

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 MIS Pupil educational files which are stored in Archive boxes	Secure user name and password **Secure archiving container on school grounds**	**25 years**
Attendance registers copies		Candidate name Candidate number	Folders	Folder is kept in a lockable filing cabinet	After post result services for that season or alternatively any appeals
Candidates' scripts		Candidate name Candidate number	Unless permissible to use in the classroom, scripts will be kept electronically in a designated folder	Folder password protected in exams officer work area only,	After post result services for that season or alternatively any appeals
Candidates' work		Candidate name Candidate Number	Return to Subject teachers after the publication of results for teachers to keep in Lockable metal filing cabinet	Exam store room while exams have finished until publication day When with subject teachers in a lockable filing cabinet. Electronic copies of work will be kept secure under password protected accounts	After post result services for that season or alternatively any appeals

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
Certificates		Candidate name Candidates Signature on collection log	Lockable filing cabinet	In secure area solely assigned to exams	Minimum of 12 months.
Certificate destruction information	.	Candidate name	In a folder stored in a lockable filing cabinet	Keeping the filing cabinet locked at all times	5 years from issue date
Certificate issue information		Candidate name Candidate signature	Lockable filing cabinet	Keeping filing cabinet locked at all times	5 years from issue date
Entry information		Candidate name Candidate number Candidate DOB Candidate UCI/ULN	In a folder stored in a lockable filing cabinet Electronic excel file	Keeping the filing cabinet locked at all times Password protect the file	After post result services for that season or alternatively any appeals
Exam room incident logs		Candidate name	In a folder Electronic scanned copy to send to examining bodies	In a lockable filing cabinet On the exam officers secure work area password protected	After post result services for that season or alternatively any appeals
Invigilator and facilitator training records		Staff names Staff signatures	in a folder (confirmation of attendance)	In a lockable file cabinet	Assessment records along with appraisals are kept for 5 years
Overnight supervision information		Candidate name Candidate's supervisor signature Head of Centre signature	In a folder Electronic scanned copy to examining body	In a lockable filing cabinet Password protected in the exam officers secure work area	After post result services for that season or alternatively any appeals
Post-results services: confirmation of candidate consent information		Candidate name Candidate signature	Signed document in a folder	Kept in a lockable filing cabinet.	After post result services for that season or alternatively any appeals

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
Post-results services: requests/outcome information		Candidate name Candidate Signature	Outcomes are updated on an excel tracking sheet Outcomes sent to pupils by post	Password protected in exam officers secure work area	To be retained until after the deadline for EARs or until any appeal, malpractice or other results enquiry has been completed, whichever is later
Post-results services: scripts provided by ATS service		Candidate name Candidate Number	Files downloaded electronically from exam board	Saved electronically in the exam officers secure work area and password protected	Until the end of the ATS service
Post-results services: tracking logs		Candidate name			To be retained until after the deadline for EARs or until any appeal, malpractice or other results enquiry has been completed, whichever is later

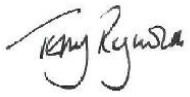
Information type	Information description (where required)	What personal/sensitive data is/may be contained in the information	Where information is stored	How information is protected	Retention period
Private candidate information		Candidate name Candidates DOB Candidate email address Candidate address Candidate UCI and/or ULN number Candidate telephone number Candidate signature	On a document in a folder	Folder kept in a lockable filing cabinet	To be retained until after the deadline for EARs or until any appeal, malpractice or other results enquiry has been completed, whichever is later
Resolving timetable clashes information		Candidate name Candidate number	File created electronically	Saved in the exam officers secure work area password protected	After post result services for that season or alternatively any appeals
Results information		Candidate name Candidate demographics (LAC/SEN etc) Candidate UCI/UPN/ULN numbers	Electronic Excel/Word /PDF/PowerPoint files	Saved secure to exam officers work area password protect Send via encrypted email to Senior staff Senior staff save to own secure work area password protect	Records for current year plus previous 6 years to be retained as a minimum.

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
Seating plans		Candidate name Invigilator signatures	Paper records kept in a folder	Kept in a lockable cabinet	To be retained until after the deadline for EARs or until any appeal, malpractice or other results enquiry has been completed, whichever is later.
Special consideration information		Candidate name Candidate sensitive information (case dependent) such as medical NHS number, scanned copy of medical letters which could include date of births and addresses, crime reference numbers etc.	Information is stored electronically – scanned PDF files	The files saved in the exam officers work area and password protected.	After post result services for that season or alternatively any appeals
Suspected malpractice reports/outcomes		Candidate name Staff signature	In a folder	In a lockable filing cabinet	After post result services for that season or alternatively any appeals
Transferred candidate arrangements		Candidate name Candidate Number Host Centre HOC/EO Signature Entering Centre HOC/EO Signature	Electronically online via JCQ secure portal	JCQ send it encrypted to exam boards	To be retained until the transfer arrangements are confirmed by the awarding body.

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
Very late arrival reports/outcomes		Candidate name Candidate Number Staff Signature	Electronically online via JCQ secure portal	JCQ send it encrypted to exam boards	After post result services for that season or alternatively any appeals

Signed:_____ Dated: December 2018_____

Head Teacher



Signed:_____ Dated: December 2018_____

Chair of Governors

Updated: October 2018