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 J Polley**
Exams Officer (Senior Leader)	**Mrs N Geater**
SENDCo	**Miss S Brosnan**
SLT member(s)	**Mr J Polley**
	Mrs N Geater
	Mr A Wilkinson
	Mr M Ashcroft (SENDCo Line Manager)
	Mr C Barnett

Purpose of the policy

This policy details how The Wensleydale School & Sixth Form, 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
- the 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;
- Management Information System (MIS) provided by Capita SIMS sending/receiving information via electronic data interchange (EDI) using A2C (https://www.jcq.org.uk/about-a2c) to/from awarding body processing systems; etc.]

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 Wensleydale School & Sixth Form ensures that candidates are fully aware of the information and data held.

All candidates are:

- informed via the annual Year 11 Exams Assembly
- given access to this policy via the centre website

Candidates are made aware of the above prior to the commencement of external 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 Laptop/tablet	April 2016 April 2016 School's ICT are responsible for checking and maintaining hardware, including backing up data securely each day, ensuring antivirus protection is up to date and that regular scans are run.	N/A N/A

Software/online system	Protection measure(s)
MIS (Capita SIMS) Go4Schools	SIMS and Go4Schools are hosted systems with data securely backed up to the Cloud in accordance with DPA and GDPR regulations. Staff are not permitted to take any hard copy information which identifies a candidate off site. Where hard copies exist, staff are held accountable for keeping the information securely in locked offices. Rules are in place regarding protected usernames and passwords and regarding access rights to individuals. The school uses the NYCC's sophisticated firewall 'Smoothwall' to protect the school's data from violation
Awarding body secure extranet site(s); A2C; etc.]	Rules are in place regarding: • protected usernames and passwords; • rules for password setting (i.e. the use of a mix of upper/lower cases letters and numbers); • rules for regularity of password changing; • new user access – the centre administrator has to approve the creation of new user accounts and determine access rights; • regular checks to Firewall/Antivirus software;
Internet browsers	The school uses the NYCC's sophisticated firewall 'Smoothwall' to protect the school's data from violation

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. Data Protection Officer services are provided to the school by NYCC Information Governance auditors 'Veritau'

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 as part of the post-exam debrief.

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
- regular updates undertaken by School's ICT (including updating antivirus software, firewalls, internet browsers etc.)

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 accessible from the 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 School Business Manager, Mrs N Geater in writing/email. Where a former candidate is unknown to current staff, the letter will need to be delivered to the school in person and with accompanying photo ID . 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, is 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**)

Record type	Record(s) description (where required)	**What personal/sensitive data is/may be contained in the information**	**Where information is stored**	**How information is protected**	Retention information/period	Action at end of retention period (method of disposal)
Access arrangements information	Any hard copy information kept by the EO relating to an access arrangement candidate.	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 Lockable metal filing cabinet	Secure user name and password Secure user name and password In secure area solely assigned to exams	To be returned to SENDCo as records owner at end of the candidate's final exam series.	Confidential waste/shredding
Attendance register copies	Duplicate Attendance Register copies not sent to exam board with scripts	Candidate name Candidate number	Exams folder in Main admin office or EO's office	Electronic lock on doors	To be retained until after EARs	Confidential waste/shredding
Awarding body administrative guides/manuals	Any hard copy publications provided by awarding bodies.				To be retained until the current academic year update is provided.	Confidential waste/shredding
Candidates' work	Non-examination assessment work (including. controlled assessment/coursework) returned to the centre after awarding body moderation.	Candidate name Candidate number Candidate signature Candidate declaration sheet	In exams cupboard	Double locked	To be returned to subject staff as records' owner after EARs. To be stored safely and securely along with work that did not form part of the moderation sample (including materials stored electronically) until after the deadline for EARs or the	Returned to candidates or safe disposal

					resolution of any outstanding enquiries/appeals or malpractice investigations for the exam series.	
Certificates		Candidate name Candidate number Candidate result	Folder in main Admin Office	Electronic lock on door	Unclaimed/uncollected certificates to be retained securely for a minimum of 12 months from date of issue.	Confidential destruction and record retained for 4 years detailing the names of the candidates whose certificates have been destroyed
Certificate destruction information	A record of unclaimed certificates that have been destroyed.	Candidate name Candidate number	Folder in main Admin Office	Electronic lock on door	To be retained for 4 years from the date of certificate destruction.	Confidential destruction
Certificate issue information	A record of certificates that have been issued to candidates.	Candidate name Candidate number	Folder in main Admin Office	Electronic lock on door	Record retained for 12 months then scanned and stored electronically on the server's J drive.	Hard copy of scanned document confidentially destroyed
Confidential materials delivery logs	A log recording confidential materials delivered by awarding bodies to the centre and issued to authorised staff.	N/A	N/A	N/A	Record retained for 12 months then scanned and stored electronically on the server's J drive.	Hard copy of scanned document confidentially destroyed
Confidential materials tracking logs	A log to track materials taken from or returned to secure storage throughout the time the material is confidential.	N/A	N/A	N/A	Record retained for 12 months then scanned and stored electronically on the server's J drive.	Hard copy of scanned document confidentially destroyed
Dispatch logs	Proof of dispatch of exam script packages to awarding body examiners covered by the DfE (Standards & Testing Agency) yellow label service	N/A	N/A	N/A	Record retained for 12 months then scanned and stored electronically on the server's J drive.	Hard copy of scanned document confidentially destroyed
Entry information	Any hard copy information relating to candidates' entries.	Candidate name Tier of entry	EO's office	Electronic door lock	Records held securely in EO until outcome of EARs	Confidentially destroyed in November
Exam question papers	Question papers for timetabled written exams.	N/A	N/A	N/A	Issued to teaching staff after the published finishing time of the exam and only when all candidates	

					in the centre have completed the exam. Instructions issued by an individual awarding body relating to the use of question papers for vocational qualifications after the examination has taken place are followed. [Reference ICE 16 and GR 6,5]	
Exam room checklists	Checklists confirming room conditions and invigilation arrangements for each exam room.	Candidate name Candidate number Location of exam room	Eo's office and/or main admin office Taken to exam room location on day of exam	Electronic door locks	To be retained until the deadline for EARs or the resolution of any outstanding enquiries/appeals for the relevant exams series. [Reference ICE 6]	Confidentially destroyed
Exam room incident logs	Logs recording any incidents or irregularities in exam rooms.	Candidate name Candidate number Details of incident	EO's office	Electronic door lock	Record retained for 12 months then scanned and stored electronically on the server's J drive.	Hard copy of scanned document confidentially destroyed
Exam stationery		N/A	N/A	N/A	When awarding body or JCQ common stationery is considered surplus or is out-of-date it will be disposed of. [Reference ICE page 4 and ICE 23]	Confidential disposal
examiner reports		Candidate number Details of who work met assessment objectives	Scanned on to secure J drive	Secure drive with access limited to EO, SLT and Faculty Leaders Hard copies securely destroyed	To be shared electronically with Faculty Leaders as records' owner as part of results sharing.	Confidential waste/shredding
Finance information	Copy invoices for exams-related fees.	N/A	N/A	N/A	To be returned to Finance department as records owner at the end of the academic year.	
Invigilation arrangements	See *Exam room checklists*	Checklists confirming room conditions and invigilation arrangements for each exam room.	Candidate name Candidate number Location of exam room	EO's office and/or main admin office – electronic door locks Taken to exam room location on day of exam	To be retained until the completion of EARs	Confidentially destroyed

JCQ publications	Any hard copy publications provided by JCQ.	N/A	N/A	N/A	To be retained until the current academic year update is provided.	Confidentially destroyed
Moderator reports	Any hard copy moderator report	Candidate number Details of who work met assessment objectives	Scanned on to secure J drive	Secure drive with access limited to EO, SLT and Faculty Leaders Hard copies securely destroyed	To be shared electronically with Faculty Leaders as records' owner as part of results sharing.	Confidential waste/shredding
Overnight supervision information	Copy of JCQ form *Timetable variation and confidentiality declaration for overnight supervision* for any candidate eligible for these arrangements.	Candidate name Candidate number Exam details Supervision details	Stored in EO's office	Electronic door lock	To be retained for JCQ inspection purposes.	Record retained for 12 months then scanned and stored electronically on the server's J drive. Hard copy of scanned document confidentially destroyed
Post-results services: confirmation of candidate consent information	Hard copy or email record of candidate consent for an EAR or ATS request to be submitted to an awarding body	Candidate name Candidate number Candidate email address Details of exams for which EAR is requested	Stored in EO's office	Electronic door lock	EAR consent to be retained for at least six months following the outcome of the enquiry or any subsequent appeal. ATS consent to be retained for at least six months from the date consent given.	Record retained for 12 months then scanned and stored electronically on the server's J drive. Hard copy of scanned document confidentially destroyed
Post-results services: requests/outcome information	Any hard copy information relating to a post-results service request (EARs, appeals, ATS) submitted to an awarding body for a candidate and outcome information from the awarding body.	Candidate name Candidate number Candidate email address Details of exams for which EAR is requested Outcomes of EAR	Stored in EO's office Shared with staff via Google Drive	Electronic door lock Secure username and password to access	Record retained for 12 months then scanned and stored electronically on the server's J drive.	Hard copy of scanned document confidentially destroyed
Post-results services: scripts returned from ATS service	Copy or original exam scripts returned to the centre by the awarding body.	Candidate name Candidate number	Scripts are password protected and stored on Google Drive and shared with the candidate and the relevant Faculty Leader (if permission	Password protected and a secure link emailed to the candidate/Faculty Leader	Where scripts are retained by the centre, they must be securely stored (including any electronic versions) and not edited in any way or disposed of until after the awarding body deadline. [Reference PRS 8]	Confidential disposal

			has been granted by the candidate)			
Post-results services: tracking logs	A log tracking to resolution all post-results service requests submitted to awarding bodies.	Candidate name Candidate number Outcome of EAR	Google Drive	Password protected	Log uploaded to Drive	Stored indefinitely
Proof of postage – candidate work	Proof of postage of sample of candidates' work to awarding body moderators.	N/A	N/A	N/A	To be kept until the deadline for EARs and the resolution of any outstanding enquiries/appeals for the relevant exams series.	Confidentially destroyed
Resolving clashes information	Any hard copy information relating to the resolution of a candidate's clash of exam papers or a timetable variation.	Candidate name Candidate number	EO's office	Electronic door lock	To be kept until the deadline for EARs and the resolution of any outstanding enquiries/appeals for the relevant exams series.	Confidentially destroyed
Results information	Broadsheets of results summarising candidate final grades by subject by exam series.	Candidate name Candidate number Candidate result	Stored in EO's office and uploaded to Google Drive with a secure link emailed to Faculty Leader/SLT	Password protected	Records for current year plus previous 6 years to be retained as a minimum. [Reference Information Management Toolkit for Schools page 52]	Records stored electronically on J drive and hard copies confidentially destroyed
Seating plans	Plans showing the seating arrangements of all candidates for every exam taken.	Candidate number Exam	Stored in EO's office	Electronic door lock	To be kept until the deadline for EARs and the resolution of any outstanding enquiries/appeals for the relevant exams series. [Reference ICE 6]	Confidentially destroyed
Special consideration information	Any hard copy information relating to a special consideration request and supporting evidence submitted to an awarding body for a candidate.	Candidate name Candidate number Details of request Supporting documentation	Stored in EO's office. Scanned and uploaded to secure J drive	Electronic door lock Secure J drive with limited access	Evidence supporting an on-line special consideration application and evidence supporting a candidate's absence from an exam must be kept until after the publication of results. [Reference SC 6]	Confidentially destroyed

Suspected malpractice reports/outcomes	Any hard copy information relating to a suspected malpractice investigation/report submitted to an awarding body and outcome information from the awarding body.	Candidate name Candidate number Details of incident Supporting documentation	Stored in EO's office. Scanned and uploaded to secure J drive	Electronic door lock Secure J drive with limited access	Retained as directed in the outcome letter including on staff personnel files where indicated	Confidentially destroyed
Transfer of credit information	Any hard copy information relating to a GCE AS transfer of credit arrangement (for a legacy unitised GCE AS specification) application submitted to an awarding body for a candidate.	Candidate name Candidate number Details of credit information	Stored in EO's office. Scanned and uploaded to secure J drive	Electronic door lock Secure J drive with limited access	To be retained until the issue of the GCE A level result for the candidate.	Confidentially destroyed
Transferred candidate information	Any hard copy information relating to an application for a transferred candidate arrangement submitted to an awarding body for a candidate.	Candidate name Candidate number Previous/current centre ID numbers	Stored in EO's office. Scanned and uploaded to secure J drive	Electronic door lock Secure J drive with limited access	To be retained until the transfer arrangements are confirmed by the awarding body.	Confidentially destroyed
Very late arrival reports/outcomes	Any hard copy information relating to a very late arrival report submitted to an awarding body for a candidate and outcome information from the awarding body.	Candidate name Candidate number Details of incident	Stored in EO's office. Scanned and uploaded to secure J drive	Electronic door lock Secure J drive with limited access	Record retained for 12 months then scanned and stored electronically on the server's J drive.	Hard copy of scanned document confidentially destroyed