Data Protection Policy (exams)

2021/22

This policy is reviewed annually to ensure compliance with current regulations

Approved/reviewed by	
Date of next review	September 2022

Key staff involved in the policy

Role	Name(s)
Head of centre	**Miss K Sherwood**
Exams officer	**Mrs A Kilby**
Exams officer line manager (Senior leader)	**Mr L Coren**
IT manager	**Mr J Gray**
Data manager	**Mrs A Phillips**

Purpose of the policy

This policy details how St Luke's Church of England 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).

> At the date of reviewing these regulations, although the UK has left the European Union the General Data Protection Regulation still has a direct effect within the UK (JCQ's General Regulations for Approved Centres (GR, 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.

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
- Multi Academy Trust

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.
- 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

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

St Luke's Church of England School ensures that candidates are fully aware of the information and data held.

All candidates are:

- informed via centre newsletter, electronic communication, centre website

- given access to this policy via centre website, written request

Candidates are made aware of the above at the start of their course of study leading to an externally accredited qualification.

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.

Candidates eligible for access arrangements are also required to provide their consent by signing the GDPR compliant JCQ candidate personal data consent form (Personal data consent, Privacy Notice (AAO) and Data Protection confirmation) before access arrangements approval applications can be processed online.

Section 3 – Hardware and software

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

a. Laptops, Pads and Data sticks must be encrypted;

b. Digital equipment must be disposed of securely;

c. Paper information that contains sensitive and personal data must be disposed of using a shredder or confidential waste bags;

d. A clear desk policy must be in operation and personal data must be securely locked away when not in use;

e. All hardcopies of personal data, along with any electronic copies stored on physical, removable media should be stored securely in a locked box, drawer, cabinet or similar;

f. Screens must be positioned appropriately so that personal data cannot be seen by the public and the screen is locked when left unattended.

g. All emails sent to external third parties outside the Trust network must be sent using encryption software - 'Egress Switch'.

h. Personal data attached to emails to be avoided where possible. Where it is feasible a link to where the personal data is stored is to be used.

i. Where Personal data is to be transferred in hardcopy form it should be passed directly to the recipient or sent using Special Delivery Mail.

j. Personal data must be handled with care at all times and should not be left unattended or on view to unauthorised employees, agents, sub-contractors or other parties at any time;

k. No personal data should be stored on any mobile device (including, but not limited to, laptops, tablets and smartphones), whether such device belongs to the School or otherwise.

l. No personal data should be stored on the computer's hard drive. It must be stored on the Trust network where the data is securely stored and encrypted;

m. All passwords used to protect personal data should not use words or phrases that can be easily guessed or otherwise compromised. All passwords must contain a combination of uppercase and lowercase letters, numbers, and symbols. All software used by the Trust is designed to require such passwords;

n. Under no circumstances should any passwords be written down or shared between any employees, agents, contractors, or other parties working on behalf of the School, irrespective of seniority or department. If a password is forgotten, it must be reset using the applicable method. IT staff do not have access to passwords;

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**

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 School shall ensure that all personal data collected and processed is kept accurate and up-to-date. The accuracy of data shall be checked when it is collected and at regular intervals thereafter. Where any inaccurate or out-of-date data is found, all reasonable steps will be taken without delay to amend or erase that data, as appropriate.

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 (this may include 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 available/accessible from the Exams Officer.

Section 7 – Access to information

(with reference to ICO information https://ico.org.uk/your-data-matters/schools/exam-results/)

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

1. Requests for information must be made in writing; which includes email, and be address to Kealey Sherwood, Head Teacher. If the initial request does not clearly identify the information required, then further enquiries will be made.

2. The identity of the requestor must be established before the disclosure of any information, and checks should also be carried out regarding proof of relationship to the child. Evidence of identity can be established by requesting production of:

- Passport
- Driving licence
- Utility bills with current address
- Birth/Marriage certificate
- P45/P60
- Credit card or mortgage statement

This list is not exhaustive

3. Any individual has the right of access to information held about them. However, with children, this is dependent upon their capacity to understand (normally age 12 or above) and the nature of the request. The Head Teacher should discuss the request with the child and take their views into account when making a decision. A child with competency to understand can refuse to contact to the request for their records. Where the child is not deemed to be competent an individual with parental responsibility or guardian shall make the decision on behalf of the child.

4. The school may make a charge for the provision of information, dependent upon the following:

- Should the information requested contain the educational record then the amount charged will be dependent upon the number of pages provided.
- Should the information requested be personal information that does not include any information contained within educational records schools can charge up to £10 to provide it.
- If the information requested is only the educational record viewing will be free, but a charge not exceeding the cost of copying the information can be made by the Principal.

5. The response time for subject access request, once officially received, is 40 days **(not working or school days but calendar days, irrespective of school holiday periods).** However, the 40 days will not commence until after receipt of fees or clarification of information sought.

6. If a request is made for exam information before results have been announced, a request will be responded to:

- within five months of the date of the request, or
- within 40 days from when the results are published (whichever is earlier).

If a request is made once exam results have been published, the individual will receive a response within one month of their request.

7. The Data Protection Act 2018 allows exemptions as to the provision of some information; **therefore, all information will be reviewed prior to disclosure.**

8. Third party information is that which has been provided buy another, such as the Policy, Local Authority, Health Care professional or another school. Before disclosing third party information consent should normally be obtained. There is still a need to adhere to the 40 days' statutory timescale.

9. Any information which may cause serious harm to the physical or mental health or emotional condition of the pupil or another should not be disclosed, nor should information that would reveal that the child is at risk of abuse, or information relating to court proceedings.

10. If there are any concerns over the disclosure of information then additional advice should be sought.

11. Where redaction (information blacked out/removed) has taken place then a full copy of the information provided should be retained in order to establish, if a complaint is made, what was redacted and why.

12. Information disclosed should be clear, thus any codes or technical terms will need to be clarified and explained. If information contained within the disclosure is difficult to read or illegible, then it should be retyped.

13. Information can be provided at the school with a member of staff on hand to help and explain matters if requested, or provided at face to face handover. The views of the applicant should be taken into account when considering the method of delivery. If postal systems have to be used, then registered/recorded mail must be used.

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, St Luke's will make reference to the ICO (Information Commissioner's Office) Schools, universities and colleges information https://ico.org.uk/your-data-matters/schools/ on Publishing exam results.

(Publishing examination results is a common and accepted practice. Many students enjoy seeing their name in print, particularly in the local press and the GDPR does not stop this happening. However, under the GDPR schools have to act fairly when publishing results, and where people have concerns about their or their child's information being published, schools must take those concerns seriously.

Schools should make sure that all pupils and their parents or guardians are aware as early as possible whether examinations results will be made public and how this will be done. Schools should also explain how the information will be published. For example, if results will be listed alphabetically, or in grade order.

In general, because a school has a legitimate reason for publishing examination results, pupils or their parents or guardians do not need to give their consent to publication. However, if you have a specific concern about publication of your results, you have the right to object. Schools should consider objections from pupils and parents before making a decision to publish. A school would need to have a good reason to reject someone's objection to publication of their 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	Sims Laptops and the Schools One drive Any hard copy information is kept by the EO and SENCo in a lockable filing cabinet.	Secure user name and password In secure office (SENCO & EO)	Refer to SENCO
Alternative site arrangements	Any hard copy information generated on an alternative site arrangement. Notifications submitted online via CAP.	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	Laptops and the Schools One drive CAP/Sims	Secure user name and password	Refer to SENCO
Attendance registers copies	Attendance register to be retained with EO	Candidate name Candidate DOB Gender Candidate Exam number	To be retained with EO Sims Awarding bodies	Secure user name and password In secure office (EO) Sent by secured mail to Awarding bodies.	To be kept until the deadline for reviews of marking has passed or until any appeal, malpractice or other results enquiry has

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
					been completed, whichever is later. Confidential disposal.
Candidates' scripts		Candidate name Candidate DOB Gender Candidate Exam number	To be retained with EO Sims Any unwanted copies of scripts returned to the centre through the Access to Scripts (ATS) service.	Secure user name and password In secure office (EO)	To be retained securely until the awarding body's earliest date for confidential disposal of unwanted scripts. Confidential disposal.
Candidates' work		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	Laptops and the Schools One drive Sims Awarding bodies	Secure user name and password Sent by secured mail to Awarding bodies.	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 resolution of any outstanding enquiry/appeal or malpractice investigations for the exam series. Returned to candidates or safe disposal.
Centre consortium arrangements for centre assessed work	Any hard copy information generated or relating to consortium arrangements for centre assessed work. Applications submitted online via CAP.	Candidate name Candidate DOB Gender Candidate Exam number	Laptops and the Schools One drive CAP/Sims	Secure user name and password	

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 certificates issued by awarding bodies. **Received by EO and issued to students on GCSE presentation evening or as requested by student. Available from reception after presentation evening**	Candidate name Candidate DOB Gender Candidate Exam number	To be retained with EO	In secure office (EO)	Unclaimed/uncollected certificates to be retained securely for a minimum of 12 months from date of issue. Any remaining certificates – all possible means of contacting student is exhausted. Certificates kept at school for 5 years allowing for further education and higher education before certificates needed for the work place. [Reference GR 5] Confidential destruction.
Certificate destruction information	A record of unclaimed certificates that have been destroyed.	Candidate name Candidate DOB Gender Candidate Exam number	To be retained with EO Laptops and the Schools One drive JCQ ICE	In secure office (EO)	To be retained for 4 years from the date of certificate destruction. [Reference GR 5] Confidential destruction.
Certificate issue information	A record of certificates that have been issued.	Candidate name Candidate DOB Gender Candidate Exam number	To be retained with EO Laptops and the Schools One drive Sims Awarding bodies	In secure office (EO)	To be kept secure with remaining certificates. Confidential destruction.

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
Conflicts of Interest records	Records demonstrating the management of Conflicts of Interest	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	To be retained with EO	In secure office (EO)	To be retained in the Secure Store until after the deadline for EARs or until any appeal, malpractice or other results enquiry has been completed, whichever is later. [Reference GR 5]
Entry information	Any hard copy information relating to candidates' entries.	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	To be retained with EO Laptops and the Schools One drive Sims Awarding bodies	Secure user name and password In secure office (EO)	To be retained in the EO office until after the deadline for EARs or until any appeal, malpractice or other results enquiry has been completed, whichever is later.
Exam room incident logs	Logs recording any incidents or irregularities in exam rooms for each exam session.	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	To be retained with EO	In secure office (EC)	To be retained until after the deadline for EARs or until any appeal, malpractice or other results enquiry has been completed, whichever is later. [Reference ICE 12]

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
Invigilator and facilitator training records		Invigilator name Invigilator DOB Gender Specialist report(s) (may also include candidate address) Evidence of normal way of working Data protection notice (candidate signature) Confidentially form References	To be retained with EO Laptops and the Schools One drive Training providers website	Secure user name and password In secure office (EO)	A record of the content of the training given to invigilators must be available for inspection and retained on file until the deadline for reviews of marking has passed or until any appeal, malpractice or other results enquiry has been completed, whichever is later.
Overnight supervision information	JCQ form Timetable variation and confidentiality declaration for overnight supervision for any candidate eligible for these arrangements.	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	Sims Laptops and the Schools One drive Any hard copy information is kept by the EO in a lockable filing cabinet.	Secure user name and password In secure office (EO)	To be retained for JCQ inspection purposes for the relevant exam series. [Reference ICE 8] Confidential destruction.
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 DOB Gender Data protection notice (candidate signature) Diagnostic testing outcome(s) Specialist report(s) (may also include candidate address)	Laptops and the Schools One drive Any hard copy information is kept by the EO in a lockable filing cabinet.	Secure user name and password In secure office (EO)	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

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
		Evidence of normal way of working			months from the date consent given. [Reference PRS 4, appendix A and B] Confidential disposal
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 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	Laptops and the Schools One drive Any hard copy information is kept by the EO in a lockable filing cabinet.	Secure user name and password In secure office (EO)	To be retained in the EO office until after the deadline for EARs or until any appeal, malpractice or other results enquiry has been completed, whichever is later. Confidential disposal
Post-results services: scripts provided by ATS service	Logs tracking to resolution all post-results service requests submitted to awarding bodies.	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	Laptops and the Schools One drive Any hard copy information is kept by the EO in a lockable filing cabinet.	Secure user name and password In secure office (EO)	Where copies of scripts are retained by the centre, they must be securely stored (including any electronic versions) until they are no longer required. [Reference PRS 6] Confidential disposal
Resolving timetable clashes information	Any hard copy information relating to the resolution of a candidate's clash of timetabled exam papers	Candidate name Candidate DOB Gender	Laptops and the Schools One drive Any hard copy information is kept by the	Secure user name and password In secure office (EO)	Where copies of timetable clashes are retained by the centre, they must be securely stored (including any electronic versions)

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
		Data protection notice (candidate signature) Diagnostic testing outcome(s) Specialist report(s) (may also include candidate address) Evidence of normal way of working	EO in a lockable filing cabinet.		until they are no longer required. Confidential disposal
Results information	Broadsheets of results summarising candidate final grades by subject by exam series.	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	Sims Laptops and the Schools One drive Any hard copy information is kept by the EO in a lockable filing cabinet.	Secure user name and password In secure office (EO)	Records for current year plus previous 6 years to be retained as a minimum which are available on the school software system.
Seating plans	Plans showing the seating arrangements of all candidates for every exam taken.	Candidate name Candidate DOB Gender Candidate Exam number	To be retained with EO Laptops and the Schools One drive Sims	Secure user name and password In secure office (EO)	To be retained until after the deadline for EARs or until any appeal, malpractice or other results enquiry has been completed, whichever is later. [Reference ICE 12] Confidential disposal
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 DOB Gender	Sims Laptops and the Schools One drive Any hard copy information is kept by the	Secure user name and password In secure office (SENCO & EO)	Evidence supporting an on-line special consideration application and evidence supporting a candidate's absence

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
		Data protection notice (candidate signature) Diagnostic testing outcome(s) Specialist report(s) (may also include candidate address) Evidence of normal way of working	EO and SENCo in a lockable filing cabinet.		from an exam must be kept until after the publication of results. [Reference SC 6] Confidential disposal
Suspected malpractice reports/outcomes	Any information relating to a suspected or actual malpractice investigation/report submitted to an awarding body and outcome information from the awarding body.	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	Sims Laptops and the Schools One drive Any hard copy information is kept by the EO in a lockable filing cabinet.	Secure user name and password In secure office (EO)	To be retained by the EO until after the deadline for EARs or until any appeal, malpractice or other results enquiry has been completed, whichever is later. Confidential disposal
Transferred candidate arrangements	Transferred candidate arrangements	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	Sims Laptops and the Schools One drive Any hard copy information is kept by the EO in a lockable filing cabinet.	Secure user name and password In secure office (EO)	To be retained until the transfer arrangements are confirmed by the awarding body.
Very late arrival reports/outcomes	Very late arrival reports/outcomes	Candidate name Candidate DOB Gender	Sims Laptops and the Schools One drive	Secure user name and password In secure office (EO)	To be retained by the EO until after the deadline for EARs or until any appeal,

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
		Data protection notice (candidate signature) Diagnostic testing outcome(s) Specialist report(s) (may also include candidate address) Evidence of normal way of working	Any hard copy information is kept by the EO in a lockable filing cabinet.		malpractice or other results enquiry has been completed, whichever is later. Confidential disposal