St Paul with St Luke CofE Primary School
Leopold Street, London E3 4LA
Tel: 0207 987 4624
Website: www.spsl.towerhamlets.sch.uk
Email: admin@spsl.towerhamlets.sch.uk
Twitter: @stpaulstluke
https://www.facebook.com/spslschool

Executive-Head: Ms Fanoula Smith

Head of School: Lauren Sharpe

Data Protection Combined Information Governance Policy 2023 – 2024

May 2023

Version no	Amendments	Approval date
1	Index, Review of Data Protection, Data Breaches, Records Management, Freedom of Information, CCTV and Surveillance	

INDEX

Section 1	Introduction to Information Governance
Section 3	Information Governance Strategy
Section 6	Data Protection
Section 17	Data Breaches
Section 24	Records Management
Section 31	Freedom of Information
Section 36	CCTV and Surveillance
Appendix 1	Retention Schedule
Appendix 2	Records Disposal Record Template
Appendix 3	Information Asset Register

The school's Data Protection Officer is:

John Person, john.pearson-hicks@london.anglican.org

The first point of contact in the event of a suspected breach in the school is:

Asma Bibi, School Business Manager, abibi34.211@lgflmail.org

1. Introduction

1.1 This document constitutes St Paul with St Luke Primary School's Information Governance Policy. It details the School's obligations and compliance with relevant legislation in relation to its handling of data. It also sets out the School's commitment to providing appropriate training and increasing awareness in this area.

1.2 This Policy pulls together all the requirements for information governance so that all School information is processed legally, securely, efficiently and effectively. Information plays a key part in the School's day to day operations and governance. Accordingly, this Policy sets out the requirements, standards and best practice that apply to the handling of all information.

1.3 Information governance is a key responsibility of each and every member of the School's community. It is essential that School staff and Governors/ Trustees familiarise themselves with this Policy and the attached appendices. This Policy and the governance it sets are also expected of any third parties handling School information.

1.4 The aim of this Policy is to support the School, comply with its legal, regulatory and contractual obligations; maintain robust corporate governance and deliver high quality education. Deliver value for money and protect the public funds. Improve the way the School handles, utilises and protects its information. Increase the School's openness, transparency and engagement with the general public.

1.5 The School holds and processes standard and sensitive data, (as described in 2.3 below) for the purposes of education provision, performance monitoring, commercial engagement, contractual obligations, research and the safeguarding.

2. Scope

2.1 This Policy covers all information held by the School or on behalf of the School whether in electronic or physical format including (but not limited to):

i) electronic data stored on and processed by fixed and portable computers and storage devices;

ii) data transmitted on networks;

iii) all paper records;

iv) Visual and photographic materials including slides and CCTV;

2.2 The following are expected to comply with the Policy:

i) all staff and governors/trustees of the School;

ii) any third parties handling, or having access to, School information including for example consultants, service providers and contractors, visitors, volunteers.

2.3 The following is the classification template in accordance with which most School data can be classified:

2.3.1 personal data - this is defined in Article 4 of the General Data Protection Regulation as any information relating to an identified or identifiable natural person (referred to as a 'data subject'), where an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person. The collection, use and retention of personal data must comply with strict conditions and such data requires special measures of protection as more particularly described in the School's Data Protection Policy;

2.3.2 sensitive personal data (also known as special categories of data) is a subset of personal data - this is defined in Article 8 of the General Data Protection Regulation as personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership; data concerning health or sex life and sexual orientation; genetic data or biometric data. Medical research data for example is likely to include some sensitive personal data. The processing of sensitive personal data is subject to additional requirements and requires additional protections also as described in more detail in the School's Data Protection Policy;

2.3.3 Non-personal data (organisational data) which can be:

i) sensitive organisational data which includes commercially sensitive planning / administrative or research data, data protected by confidentiality

agreements, legally privileged information, etc. This data should be protected by appropriate protection measures; and

ii) non-sensitive organisational data which is data pertaining to School not published by default, but which may be disclosed (subject to legal advice) in response to requests made under the Freedom of Information Act.

3. INFORMATION GOVERNANCE STRATEGY

3.1 Purpose

3.1.1 The aim of this document is to enable the School to meet its information management and security responsibilities so that customers, businesses, partners and suppliers have the confidence that information is handled and stored with due regard to its value and risk. Individuals must understand the importance of using information correctly, of sharing it lawfully and of protecting it from improper use.

3.1.2 The intention of this strategy is also to enable the School to meet its legal and ethical obligations in terms of:

i) the use and security of personal identifiable information;

ii) appropriate disclosure of information when required;

iii) regulatory Policies for the management of information;

iv) professional codes of conduct for consent to the recording, sharing and uses of information;

v) operating procedures and codes of practice adopted by the School;

vi) information exchanged with third parties.

3.1.3 The strategy recognises the high standards expected of the School as well as the ongoing task of maintaining appropriate standards of security in the area of information governance and of embedding a security culture fully throughout the School.

3.2 Strategic objectives

3.2.1 These are the overarching information governance objectives of the School. We want:

i) the infrastructure and processes for service delivery to provide the right information to the right people at the right time for the right purpose and

promote the provision of high quality services by promoting the ethical, legal, effective and appropriate use of information;

ii) to promote information governance ensuring that it is embedded throughout the school and to direct cultural change so that information is regarded as a key asset;

iii) to build into staff competencies and job descriptions specific requirements around the governance of information;

iv) to encourage staff to work closely together, preventing duplication of effort and enabling more efficient use of resources;

v) to work to achieve required standards to comply with legislative, regulatory and contractual obligations and relevant policies;

vi) to identify and manage information assets across School;

vii) to implement and operate proportionate controls that apply best practice standards to protect information assets and give confidence to all interested parties;

viii) to provide adequate training to all staff, increase awareness and embed a culture of care and responsibility in the handling of all information throughout the School.

3.3 Approach

3.3.1 Information governance and assurance are integrated into all aspects of School operations. In delivering information governance services, four key elements of School operations will be considered:

i) people

ii) process

iii) information

iv) technology

3.3.2 All information governance, improvement and assurance activities will consider how these factors need to operate in combination to achieve our strategic objectives.

3.4 Benefits

3.4.1 The following benefits (which are not an exhaustive list) provide an overview of the main benefits that should be derived through the delivery of this strategy:

i) consistent and effective management of information across the School;

ii) increased understanding of and compliance with relevant legislation;

iii) reduced number of information security incidents;

iv) reduced staff time and effort;

v) improved data quality;

vi) clear responsibilities in relation to Information Governance and Assurance;

vii) effective management of information risks;

viii) greater confidence that information risks are effectively managed;

3.5 Governance

3.5.1 The School Governors along with the Head Teacher are responsible for implementing this policy.

4. Policies

4.1 This Information Governance Policy incorporates the following individual policies:

i) Data Protection Policy

ii) Breach Policy

iii) Records Management Policy

iv) Freedom of Information Policy

v) CCTV Policy

vi) Information Asset Register

5. Training and development

5.1 Information governance training and development is essential for the development and improvement of staff knowledge and skills relating to information governance across the School.

5.2 Information governance training must extend beyond basic confidentiality and security awareness in order to develop and follow best practice. Staff must understand the

value of information and their responsibility for it, which includes data quality, information security, records management, confidentiality, etc.

5.3 Information governance basic awareness is a mandatory requirement for all new staff as part of their induction.

6. DATA PROTECTION

6. St Paul with St Luke Primary School collects and uses certain types of personal information about staff, pupils, parents and other individuals who come into contact with the school in order provide education and associated functions. The school may be required by law to collect and use certain types of information to comply with statutory obligations related to employment, education and safeguarding, and this policy is intended to ensure that personal information is dealt with properly and securely and in accordance with the General Data Protection Regulation and other related legislation.

6.1 GDPR applies to all computerised data and manual files if they come within the definition of a filing system. Broadly speaking, a filing system is one where the data is structured in some way that it is searchable on the basis of specific criteria (so you would be able to use something like the individual's name to find their information), and if this is the case, it does not matter whether the information is located in a different physical location.

7. Personal Data

7.1 The School is the Data Controller for personal data (as defined in 2.3.1) and special category data (as defined in 2.3.2)

7.2 Information relating to criminal convictions will only be held and processed where there is legal authority to do so.

7.3 St Paul with St Luke Primary School does not intend to seek or hold sensitive personal data about staff or students except where the School has been notified of the information, or it comes to the school's attention via legitimate means (e.g. a grievance) or needs to be sought and held in compliance with a legal obligation or as a matter of good practice. Staff, Parents/ Carers, Students and Governors/Trustees are under no obligation to disclose to the school their race or ethnic origin, political or religious beliefs, whether or not they are a trade union member or details of their sexual life (save to the extent that details of marital status and / or parenthood are needed for other purposes, e.g. pension entitlements).

8. The Data Protection Principles

8.1 The six data protection principles as laid down in the GDPR are followed by The School at all times:

i) First Principle, personal data shall be processed fairly, lawfully and in a transparent manner, and processing shall not be lawful unless one of the processing conditions can be met;

ii) Second Principle, personal data shall be collected for specific, explicit, and legitimate purposes, and shall not be further processed in a manner incompatible with those purposes;

iii) Third Principle, personal data shall be adequate, relevant, and limited to what is necessary for the purpose(s) for which it is being processed;

iv) Fourth Principle, personal data shall be accurate and, where necessary, kept up to date;

v) Fifth Principle, personal data processed for any purpose(s) shall not be kept for longer than is necessary for that purpose / those purposes;

vi) Sixth Principle, personal data shall be processed in such a way that ensures appropriate security of the data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.

8.2 In addition to this, St Paul with St Luke is committed to ensuring that at all times, anyone dealing with personal data shall be mindful of the individual's rights under the law (as explained in more detail in sections 14 and 16 below).

8.3 St Paul with St Luke is committed to complying with the principles in 8.1 at all times. This means that the School will:

i) inform individuals as to the purpose of collecting any information from them, as and when we ask for it;

ii) be responsible for checking the quality and accuracy of the information;

iii) regularly review the records held to ensure that information is not held longer than is necessary, and that it has been held in accordance with the data retention policy;

iv) ensure that when information is authorised for disposal it is done appropriately;

v) ensure appropriate security measures to safeguard personal information whether it is held in paper files or on our computer system, and follow the relevant security policy requirements at all times;

vi) share personal information with others only when it is necessary and legally appropriate to do so;

vii) set out clear procedures for responding to requests for access to personal information known as subject access requests;

viii) report any breaches of the GDPR in accordance with the procedure in paragraph 9 below.

9. Conditions for Processing Data under the First Principle

9.1 The School will ensure that when processing data under the first Data Protection Principle, they meet one of the following conditions:-

i) The individual has given consent that is specific to the particular type of processing activity, and that consent is informed, unambiguous and freely given.

ii) The processing is necessary for the performance of a contract, to which the individual is a party, or is necessary for the purpose of taking steps with regards to entering into a contract with the individual, at their request.

iii) The processing is necessary for the performance of a legal obligation to which we are subject.

iv) The processing is necessary to protect the vital interests of the individual or another.

v) The processing is necessary for the performance of a task carried out in the public interest, or in the exercise of official authority vested in us.

10. Use of Personal Data by St Paul with St Luke

10.1 St Paul with St Luke holds personal data on pupils, staff and other individuals such as visitors. In each case, the personal data must be treated in accordance with the data protection principles as outlined in paragraph 8.1 above.

Pupils

10.2 The personal data held regarding pupils includes contact details, assessment / examination results, attendance information, characteristics such as ethnic group, special educational needs, any relevant medical information, and photographs.

10.3 The data is used in order to support the education of the pupils, to monitor and report on their progress, to provide appropriate pastoral care, and to assess how well as a whole is doing, together with any other uses normally associated with this provision in a school environment.

10.4 St Paul with St Luke may make use of limited personal data (such as contact details) relating to pupils, and their parents or guardians for fundraising, marketing or promotional purposes and to maintain relationships with pupils of the School, but only where consent has been provided to this.

10.5 In particular, St Paul with St Luke may:

i) transfer information to any association society or club set up for the purpose of maintaining contact with pupils or for fundraising, marketing or promotional purposes relating to but only where consent has been obtained first

ii) make personal data, including sensitive personal data, available to staff for planning curricular or extra-curricular activities;

iii) Use photographs of pupils in accordance with the photograph policy.

iv) Any wish to limit or object to any use of personal data should be notified to the Data Protection Officer (DPO) in writing, which will be acknowledged by in writing. If, in the view of the DPO the objection cannot be maintained, the individual will be given written reasons why cannot comply with their request.

Staff

10.6 The personal data held about staff will include contact details, employment history, information relating to career progression, information relating to DBS checks, photographs.

10.7 The data is used to comply with legal obligations placed on St Paul with St Luke in relation to employment, and the education of children in a school environment. The school may pass information to other regulatory authorities where appropriate, and may use names and photographs of staff in publicity and promotional material with their consent. Personal data will also be used when giving references.

10.8 Staff should note that information about disciplinary action may be kept for longer than the duration of the sanction. Although treated as "spent" once the period of the sanction has expired, the details of the incident may need to be kept for a longer period.

10.9 Any wish to limit or object to the uses to which personal data is to be put should be notified to the DPO who will ensure that this is recorded, and adhered to if appropriate. If the DPO is of the view that it is not appropriate to limit the use of personal data in the way specified, the individual will be given written reasons why cannot comply with their request.

Other Individuals

10.10 St Paul with St Luke may hold personal information in relation to other individuals who have contact with the school, such as volunteers and visitors. Such information shall be held only in accordance with the data protection principles, and shall not be kept longer than necessary.

11. Security of Personal Data

11.1 St Paul with St Luke will take reasonable steps to ensure that members of staff will only have access to personal data where it is necessary for them to carry out their duties. All staff will be made aware of this and their duties at Induction.

11.2 St Paul with St Luke will take all reasonable steps to ensure that all personal information is held securely and is not accessible to unauthorised persons.

12. Disclosure of Personal Data to Third Parties

12.1 The following list includes the most usual reasons that the School will authorise disclosure of personal data to a third party:

i) To give a confidential reference relating to a current or former employee, volunteer or pupil;

ii) for the prevention or detection of crime;

iii) for the assessment of any tax or duty;

iv) where it is necessary to exercise a right or obligation conferred or imposed by law upon (other than an obligation imposed by contract);

v) for the purpose of, or in connection with, legal proceedings (including prospective legal proceedings);

vi) for the purpose of obtaining legal advice;

vii) for research, historical and statistical purposes (so long as this neither supports decisions in relation to individuals, nor causes substantial damage or distress);

viii) to publish the results of public examinations or other achievements of pupils of ;

ix) to disclose details of a pupil's medical condition where it is in the pupil's interests to do so, for example for medical advice, insurance purposes or to organisers of school trips;

x) to provide information to another educational establishment to which a pupil is transferring;

xi) to provide information to the Examination Authority as part of the examination process; and

xii) to provide information to the relevant Government Department concerned with national education. At the time of the writing of this Policy, the Government Department concerned with national education is the Department for Education (DfE). The Examination Authority may also pass information to the DfE.

12.2 The DfE uses information about pupils for statistical purposes, to evaluate and develop education policy and to monitor the performance of the nation's education service as a whole. The statistics are used in such a way that individual pupils cannot be identified from them. On occasion the DfE may share the personal data with other Government Departments or agencies strictly for statistical or research purposes.

12.3 St Paul with St Luke may receive requests from third parties (i.e. those other than the data subject, (or their representative) to disclose personal data it holds about pupils, their parents or guardians, staff or other individuals. This information will not generally be disclosed unless one of the specific exemptions under data protection legislation which allow disclosure applies; or where necessary for the legitimate interests of the individual concerned.

12.4 All requests for the disclosure of personal data must be sent to the DPO who will review and decide whether to make the disclosure, ensuring that reasonable steps are taken to verify the identity of that third party before making any disclosure.

13 Confidentiality of Pupil Concerns

13.1 Where a pupil seeks to raise concerns confidentially with a member of staff and expressly withholds their agreement to their personal data being disclosed to their parents or guardian, will maintain confidentiality unless it has reasonable grounds to believe that the pupil does not fully understand the consequences of withholding their consent, or where believes disclosure will be in the best interests of the pupil or other pupils.

14 Subject Access Requests

14.1 Anybody who makes a request to see any personal information held about them by is making a subject access request. All information relating to the individual, including that held in electronic or manual files should be considered for disclosure, provided that they constitute a "filing system".

14.2 All requests should be sent to the DPO within 3 working days of receipt, and must be dealt with in full without delay and at the latest within one month of receipt.

14.3 Where a child or young person does not have sufficient understanding to make his or her own request (usually those under the age of 13, or over 13 but with a special educational need which makes understanding their information rights more difficult), a person with parental responsibility can make a request on their behalf. The DPO must, however, be satisfied that:

i) the child or young person lacks sufficient understanding; and

ii) the request made on behalf of the child or young person is in their interests.

14.4 Any individual, including a child or young person with ownership of their own information rights, may appoint another person to request access to their records. In such circumstances must have written evidence that the individual has authorised the person to make the application and the DPO must be confident of the identity of the individual making the request and of the authorisation of the individual to whom the request relates.

14.5 Access to records will be refused in instances where an exemption applies, for example, information sharing may place the individual at risk of significant harm or jeopardise police investigations into any alleged offence(s).

14.6 An individual only has the automatic right to access information about themselves, and care needs to be taken not to disclose the personal data of third parties where consent has not been given, or where seeking consent would not be reasonable, and it would not be appropriate to release the information. Particular care must be taken in the case of any complaint or dispute to ensure confidentiality is protected.

14.7 All files must be reviewed by the DPO before any disclosure takes place. Access will not be granted before this review has taken place.

14.8 Where all the data in a document cannot be disclosed a permanent copy should be made and the data obscured or retyped if this is more sensible. A copy of the full document and the altered document should be retained, with the reason why the document was altered.

15 Exemptions to Access by Data Subjects or their Representative

15.1 Where a claim to legal professional privilege could be maintained in legal proceedings, the information is likely to be exempt from disclosure unless the privilege is waived.

15.2 There are other exemptions from the right of subject access. If we intend to apply any of them to a request then we will usually explain which exemption is being applied and why.

16 Other Rights of Individuals

16.1 St Paul with St Luke has an obligation to comply with the rights of individuals under the law, and takes these rights seriously. The following section sets out how will comply with the rights to:

i) object to Processing;

ii) rectification;

iii) erasure; and

iv) data Portability.

16.2 Right to object to processing

16.2.1 An individual has the right to object to the processing of their personal data on the grounds of pursuit of a public interest or legitimate interest (grounds 4.5 and 4.6 above) where they do not believe that those grounds are made out.

16.2.2 Where such an objection is made, it must be sent to the DPO within 2 working days of receipt, and the DPO will assess whether there are compelling legitimate grounds to continue processing which override the interests, rights and freedoms of the individuals, or whether the information is required for the establishment, exercise or defence of legal proceedings.

16.2.3 The DPO shall be responsible for notifying the individual of the outcome of their assessment within fourteen working days of receipt of the objection.

16.3 Right to rectification

16.3.1 An individual has the right to request the rectification of inaccurate data without undue delay. Where any request for rectification is received, it should be sent to the DPO within 2 working days of receipt, and where adequate proof of inaccuracy is given, the data shall be amended as soon as reasonably practicable, and the individual notified.

16.3.2 Where there is a dispute as to the accuracy of the data, the request and reasons for refusal shall be noted alongside the data, and communicated to the individual. The individual shall be given the option of [a review under the data protection complaints procedure, or an appeal direct to the Information Commissioner.

16.3.3 An individual also has a right to have incomplete information completed by providing the missing data, and any information submitted in this way shall be updated without undue delay.

16.4 Right to erasure

16.4.1 Individuals have a right, in certain circumstances, to have data permanently erased without undue delay. This right arises in the following circumstances:

i) where the personal data is no longer necessary for the purpose or purposes for which it was collected and processed;

ii) where consent is withdrawn and there is no other legal basis for the processing;

iii) where an objection has been raised under the right to object, and found to be legitimate;

iv) where personal data is being unlawfully processed (usually where one of the conditions for processing cannot be met);

v) where there is a legal obligation on to delete.

16.4.2 The DPO will make a decision regarding any application for erasure of personal data, and will balance the request against the exemptions provided for in the law. Where a decision is made to erase the data, and this data has been passed to other data controllers, and / or has been made public, reasonable attempts to inform those controllers of the request shall be made.

16.5 Right to restrict processing

16.5.1 In the following circumstances, processing of an individual's personal data may be restricted:

i) where the accuracy of data has been contested, during the period when is attempting to verify the accuracy of the data;

ii) where processing has been found to be unlawful, and the individual has asked that there be a restriction on processing rather than erasure;

iii) where data would normally be deleted, but the individual has requested that their information be kept for the purpose of the establishment, exercise or defence of a legal claim;

iv) where there has been an objection made under para 8.2 above, pending the outcome of any decision.

16.6 Right to portability

16.6.1 If an individual wants to send their personal data to another organisation they have a right to request that St Paul with St Luke provides their information in a structured, commonly used, and machine readable format. As this right is limited to situations where St Paul with St Luke is processing the information on the basis of consent or performance of a contract, the situations in which this right can be exercised will be quite limited. If a request for this is made, it should be forwarded to the DPO within 2 working days of receipt, and the DPO will review and revert as necessary.

17 DATA BREACHES

17.1 GDPR aims to protect the rights of individuals about whom data is obtained, stored, processed or supplied and requires that organisations take appropriate security measures against unauthorised access, alteration, disclosure or destruction of personal data.

17.2 GDPR places obligations on staff to report actual or suspected data breaches and St Paul with St Luke's procedure for dealing with breaches is set out below.

17.3 Third Parties who process data on behalf of St Paul with St Luke will be required to notify the School of any data breach immediately they become aware of one.

17.4 Failure to notify the relevant individuals of a breach or suspected breach in line with this policy may be considered a disciplinary offence and appropriate action will be taken.

18. Responsible Parties

18.1 The School Data Protection Officer (DPO) has overall responsibility for breach notification within the School. They are responsible for ensuring breach notification processes are adhered to by all staff and are the designated point of contact for personal data breaches.

18.2 Asma Bibi is the first point of contact at St Paul with St Luke in the event of a suspected breach within the school.

19 Procedure

19.1 A data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data or special category data transmitted, stored or otherwise processed.

19.1.1 Examples of a data breach could include the following (but are not exhaustive): -

i) Loss or theft of data or equipment on which data is stored, for example loss of a laptop or a paper file (this includes accidental loss);

ii) Inappropriate access controls allowing unauthorised use;

iii) Equipment failure;

iv) Human error (for example sending an email or SMS to the wrong recipient);

v) Unforeseen circumstances such as a fire or flood;

vi) Hacking, phishing and other "blagging" attacks where information is obtained by deceiving whoever holds it.

19.2 The School must notify the ICO (Information Commissioner's Office) of a data breach where it is likely to result in a risk to the rights and freedoms of individuals. This means that the breach needs to be more than just losing personal data and if unaddressed the breach is likely to have a significant detrimental effect on individuals.

19.2.1 Examples of where the breach may have a significant effect includes: -

i) potential or actual discrimination;

ii) potential or actual financial loss;

iii) potential or actual loss of confidentiality;

iv) risk to physical safety or reputation;

v) exposure to identity theft (for example through the release of non-public identifiers such as passport details);

vi) the exposure of the private aspect of a person's life becoming known by others.

19.2.2 If the breach is likely to result in a high risk to the rights and freedoms of individuals then the individuals must also be notified directly.

19.3 If you know or suspect a personal data breach has occurred or may occur which meets the criteria above, you should contact the named contact for the school identified in 18.2

19.4 Breach reporting is encouraged throughout the School and staff are expected to seek advice if they are unsure as to whether the breach should be reported and/or could result in a risk to the rights and freedom of individuals.

19.5 Once reported, you should not take any further action in relation to the breach. In particular you must not notify any affected individuals or regulators or investigate further.

19.6 On being notified of a suspected personal data breach, the named contact for the school identified in 18.2 will notify the DPO. They will take immediate steps to establish whether a personal data breach has in fact occurred. If so they will take steps to:-

i) Where possible, contain the data breach;

ii) As far as possible, recover, rectify or delete the data that has been lost, damaged or disclosed;

iii) Assess and record the breach in the School's data breach register;

iv) Notify the ICO;

v) Notify data subjects affected by the breach;

vi) Notify other appropriate parties to the breach;

vii) Take steps to prevent future breaches.

19.7 The DPO will notify the ICO when a personal data breach has occurred which is likely to result in a risk to the rights and freedoms of individuals. This will be done without undue delay and, where possible, within 72 hours of becoming aware of the breach. If the School are unsure of whether to report a breach, the assumption will be to report it.

19.8 Where the notification is not made within 72 hours of becoming aware of the breach, written reasons will be recorded as to why there was a delay in referring the matter to the ICO

19.9 Where the data breach is likely to result in a high risk to the rights and freedoms of data subjects, the DPO will notify the affected individuals without undue delay including the name and contact details of the ICO, the likely consequences of the data breach and the measures the School have (or intended) to take to address the breach.

19.10 When determining whether it is necessary to notify individuals directly of the breach, the named contact for the school identified in 18.2 will work with the DPO, the ICO and any other relevant authorities (such as the police).

19.11 If it would involve disproportionate effort to notify the data subjects directly (for example, by not having contact details of the affected individual) then the School will consider alternative means to make those affected aware (for example by making a statement on the School website).

20. Notifying Other Authorities

20.1 The School will need to consider whether other parties need to be notified of the breach. For example: -

i) Insurers;

ii) Parents;

iii) Third parties (for example when they are also affected by the breach);

iv) Local authority;

v) The police (for example if the breach involved theft of equipment or data). This list is non-exhaustive.

21. Assessing the Breach

21.1 Once initial reporting procedures have been carried out, the School will carry out all necessary investigations into the breach.

21.2 The School will identify how the breach occurred and take immediate steps to stop or minimise further loss, destruction or unauthorised disclosure of personal data. We will identify ways to recover correct or delete data (for example notifying our insurers or the police if the breach involves stolen hardware or data).

21.3 Having dealt with containing the breach, the School will consider the risks associated with the breach. These factors will help determine whether further steps need to be taken (for example notifying the ICO and/or data subjects as set out above). These factors include: -

i) What type of data is involved and how sensitive it is;

ii) The volume of data affected;

iii) Who is affected by the breach (i.e. the categories and number of people involved);

iv) The likely consequences of the breach on affected data subjects following containment and whether further issues are likely to materialise;

v) Are there any protections in place to secure the data (for example, encryption, password protection, pseudonymisation);

vi) What has happened to the data;

vii) What could the data tell a third party about the data subject;

viii) What are the likely consequences of the personal data breach on the school; and

ix) Any other wider consequences which may be applicable.

22. Preventing Future Breaches

22.1 Once the data breach has been dealt with, the School will consider its security processes with the aim of preventing further breaches. In order to do this, we will: -

i) Establish what security measures were in place when the breach occurred;

ii) Assess whether technical or organisational measures can be implemented to prevent the breach happening again;

iii) Consider whether there is adequate staff awareness of security issues and look to fill any gaps through training or tailored advice;

iv) Consider whether its necessary to conduct a privacy or data protection impact assessment;

v) Consider whether further audits or data protection steps need to be taken;

vi) To update the data breach register;

vii) To debrief governors/management following the investigation.

23. Reporting Data Protection Concerns

23.1 If an individual has a concern in relation to the way data is processed within the school or by a third party the school has a contract with, it is important that these concerns are raised the named contact for the school identified in 18.2

24. Records Management

24.1 Records Disposal is the process by which St Paul with St Luke manages the 'records' held, whether in electronic format or paper

25. Retention Periods

25.1 In line with Article 5(1)(e) of the GDPR St Paul with St Luke will not retain Data in an identifiable form for any longer than necessary. In determining an appropriate retention period St Paul with St Luke will take into account any applicable statutory limitation periods and any relevant guidance documents.

25.2 The School will undertake an Annual review of electronic and paper records to ensure they are retained in line with the School Retention Document.

26 Default Periods

26.1 The default period is the minimum period for which St Paul with St Luke will retain Data. At the conclusion of the default period St Paul with St Luke will review the Data being held and determine whether it can be destroyed.

26.2 The standard default period for retaining Data will be as set out in the School Retention Document and will be recorded on the School Information Asset Register.

26.3 St Paul with St Luke will take into account the matters set out in Section 26 below in determining whether Data will be retained beyond the default period.

27 Exceptions to the Default Period

27.1 In the majority of cases Data will be securely disposed of when it reaches the end of the retention period. When assessing whether Data should be retained beyond the retention period [School Name] will consider whether:

i) The Data is subject to a current request pursuant to the GDPR.

ii) St Paul with St Luke is the subject of, or involved in ongoing legal action to which the Data is or may be relevant.

iii) The Data is or could be needed in connection with an ongoing investigation.

iv) The Data is processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, and St Paul with St Luke has put in place appropriate technical and organisational measures.

v) There are changes to the regulatory or statutory framework which require the Data to be retained for a longer period.

vi) The data subject has exercised their right to restrict the processing of the Data in accordance with Article 18 of the GDPR.

28. Disposal of Data

28.1 When Data identified for disposal is destroyed, a register of the Data destroyed will be kept (see Appendices). The destruction of Data is an irreversible act and must be clearly documented. All Data identified for disposal will be destroyed under confidential conditions by St Paul with St Luke.

28.2 St Paul with St Luke may sub-contract to another organisation its obligations to dispose of Data under confidential conditions. The school satisfy itself of the sub-contractor/third party's experience and competence to do so.

29. Manual Records

29.1 Where Data is held in paper or other manual form, the default period for retaining Data has expired and none of the exceptions for retaining Data beyond the default period at set out at Section 26 are satisfied, St Paul with St Luke will ensure the Data is shredded or otherwise confidentially disposed of by St Paul with St Luke or by a person duly authorised by St Paul with St Luke to confidentially destroy the Data.

30 Electronic Records

30.1 Where Data is held in an electronic format St Paul with St Luke will where feasible use its reasonable endeavours to:

i) Put the Data beyond use so that the Data is no longer on a live electronic system and cannot be accessed by a Data Processor.

ii) Permanently delete the Data from St Paul with St Luke electronic systems when and where this becomes possible St Paul with St Luke will only engage Data Processors that are able to provide sufficient guarantees in relation to the secure disposal of Data.

31. Freedom Of Information

31.1 St Paul with St Luke is subject to the Freedom of Information Act 2000 (FOI) as a public authority, and as such, must comply with any requests for information in accordance with the principles laid out in the Act.

31.2 Any request for any information from St Paul with St Luke is technically a request under the FOI, whether or not the individual making the request mentions the FOI. Examples of requests are:-

i) Copies of non confidential Minutes

ii) Statistical data

iii) Financial/ Budget data

iv) Staffing data

v) Contract data

31.3 In all non-routine cases, if the request is simple and the information is to be released, then the individual who received the request can release the information, but must ensure that this is done within the timescale set out below. A copy of the request and response should then be sent to the DPO (Data Protection Officer).

31.4 All other requests should be referred in the first instance to the DPO], who may allocate another individual to deal with the request. This must be done promptly, and in any event within 3 working days of receiving the request.

31.5 When considering a request under FOI, you must bear in mind that release under FOI is treated as release to the general public, and so once it has been released to an individual, anyone can then access it, and you cannot restrict access when releasing by marking the information "confidential" or "restricted".

32 Time Limit for Compliance

32.1 St Paul with St Luke must respond as soon as possible, and in any event, within 20 working days of the date of receipt of the request. When calculating the 20 working day deadline, a "working day" is a school day (one in which pupils are in attendance), subject to an absolute maximum of 60 normal working days (not school days) to respond.

33 Procedure for dealing with a request

33.1 When a request is received that cannot be dealt with by simply providing the information, it should be referred in the first instance to the DPO who may re-allocate to an individual with responsibility for the type of information requested.

33.2 The first stage in responding is to determine whether or not "holds" the information requested. St Paul with St Luke will hold the information if it exists in computer or paper format. Some requests will require to take information from different sources and manipulate it in some way. Where this would take minimal effort, is considered to "hold" that information, but if the required manipulation would take a significant amount of time, the requestor should be contacted to explain that the information is not held in the manner requested, and offered the opportunity to refine their request. For example, if a request

required to add up totals in a spread sheet and release the total figures, this would be information "held" by. If a request would have to go through a number of spread sheets and identify individual figures and provide a total, this is likely not to be information "held" by St Paul with St Luke, depending on the time involved in extracting the information.

33.3 The second stage is to decide whether the information can be released, or whether one of the exemptions set out in the Act applies to the information. Common exemptions that might apply include:

i) Section 40 (1) – the request is for the applicant's personal data. This must be dealt with under the subject access regime in the DPA, detailed in paragraph 9 of the DPA policy above;

ii) Section 40 (2) – compliance with the request would involve releasing third party personal data, and this would be in breach of the DPA principles as set out in paragraph 3.1 of the DPA policy above;

iii) Section 41 – information that has been sent to (but not own information) which is confidential;

iv) Section 21 – information that is already publicly available, even if payment of a fee is required to access that information;

v) Section 22 – information that St Paul with St Luke intends to publish at a future date;

vi) Section 43 – information that would prejudice the commercial interests of St Paul with St Luke and /or a third party;

vii) Section 38 – information that could prejudice the physical health, mental health or safety of an individual (this may apply particularly to safeguarding information);

viii) Section 31 – information which may prejudice the effective detection and prevention of crime – such as the location of CCTV cameras;

ix) Section 36 – information which, in the opinion of the chair of governors of St Paul with St Luke, would prejudice the effective conduct of the school . There is a special form for this on the ICO's website to assist with the obtaining of the chair's opinion.

33.4 Sections 22, 43, 31 and 36 are qualified exemptions. This means that even if the exemption applies to the information, you also have to carry out a public interest weighting exercise, balancing the public interest in the information being released, as against the public interest in withholding the information.

35 Responding to a request

35.1 When responding to a request where St Paul with St Luke has withheld some or all of the information, must explain why the information has been withheld, quoting the appropriate section number and explaining how the information requested fits within that exemption. If the public interest test has been applied, this also needs to be explained.

35.2 The letter should end by explaining to the requestor how they can complain – either by reference to an internal review by a governor, or by writing to the ICO.

36. CCTV

36.1 At St Paul with St Luke, we take our responsibility towards the safety of staff, visitors and pupils very seriously. To that end, we use surveillance cameras to monitor any instances of aggression or physical damage to our school and its members.

36.2 The images that are captured only used for the purposes we require them for.

36.3 We reassure those persons whose images are being captured, that the images are being handled in accordance with data protection legislation.

36.4 The School's use of CCTV will capture moving and still images of people who could be identified, as well as information relating to individuals for any of the following purposes:

i) Observing what an individual is doing

ii) Taking action to prevent a crime

iii) Using images of individuals that could affect their privacy

37 Legal framework

37.1 The use of CCTV has due regard to legislation and statutory guidance, including, but not limited to the following:

i) The Regulation of Investigatory Powers Act 2000

ii) The Protection of Freedoms Act 2012

iii) The General Data Protection Regulation (GDPR)

iv) The Data Protection Act 2018

v) The Freedom of Information Act 2000

vi) The Education (Pupil Information) (England) Regulations 2005 (as amended in 2016)

vii) The School Standards and Framework Act 1998

viii) The Children Act 1989

ix) The Children Act 2004

x) The Equality Act 2010

38. Definitions

38.1 For the purpose of the use of CCTV a set of definitions will be outlined, in accordance with the surveillance code of conduct.

i) Surveillance – monitoring the movements and behaviour of individuals; this can include video, audio or live footage. For the purpose of this policy only video and audio footage will be applicable.

ii) Covert surveillance – any use of surveillance which is intentionally not shared with the subjects it is recording. Subjects will not be informed of such surveillance.

38.2 St Paul with St Luke does not condone the use of covert surveillance when monitoring any visitors to the school

39. St Paul with St Luke, is the data controller. The governing board of St Paul with St Luke therefore has overall responsibility for ensuring that records are maintained, including security and access arrangements in accordance with regulations.

39.1 The role of the data controller includes.

i) Processing surveillance and CCTV footage legally and fairly.

ii) Collecting surveillance and CCTV footage for legitimate reasons and ensuring that it is used accordingly.

iii) Collecting surveillance and CCTV footage that is relevant, adequate and not excessive in relation to the reason for its collection.

iv) Ensuring that any surveillance and CCTV footage identifying an individual is not kept for longer than is necessary.

v) Protecting footage containing personal data against accidental, unlawful destruction, alteration and disclosure – especially when processing over networks.

40. Purpose and justification

40.1 The school will only use surveillance cameras for the safety and security of the school and its staff, pupils and visitors.

40.2 Surveillance will be used as a deterrent for violent behaviour and damage to the school.

40.3 The school will only conduct surveillance as a deterrent and under no circumstances will the surveillance and the CCTV cameras be used for routine monitoring of staff.

41. St Paul with St Luke will only collect CCTV in line with the Data Protection Principles as set out in Section 8

42 Objectives of the use of CCTV

42.1 The surveillance system will be used to:

i) Maintain a safe environment

ii) Ensure the welfare of pupils, staff and visitors

iii) Deter criminal acts against persons and property.

iv) Assist the police in identifying persons who have committed an offence.

43. Protocols

43.1 The surveillance system will be registered with the ICO in line with data protection legislation.

43.2 The surveillance system is a closed digital system which does not record audio.

43.3 Warning signs have been placed at the entrances to the premises where the surveillance system is active, as mandated by the ICO's Code of Practice.

43.4 The surveillance system has been designed for maximum effectiveness and efficiency; however, the school cannot guarantee that every incident will be detected or covered and 'blind spots' may exist.

43.5 The surveillance system will not be trained on individuals unless an immediate response to an incident is required.

43.6 The surveillance system will not be trained on private vehicles or property outside the perimeter of the school.

44. Security

44.1 Access to the surveillance system, software and data will be strictly limited to authorised operators and will be password protected.

44.2 The main control facility is kept secure and locked when not in use.

44.3 Surveillance and CCTV systems will be tested for security flaws annually to ensure that they are being properly maintained at all times.

44.4 Any cameras that present faults will be repaired immediately as to avoid any risk of a data breach.

44.5 The CCTV system can only be accessed by identified members of staff in the course of their employment

45. Privacy by design

45.1 Any changes to the use of surveillance cameras and CCTV will be subject to a Data Privacy Impact Assessment (DPIA)

45.2 A DPIA will be reviewed prior to the installation of any additional surveillance and CCTV system equipment.

45.3 If the DPIA reveals any potential security risks or other data protection issues, the school will ensure they have provisions in place to overcome these issues.

45.4 The school will ensure that the installation of the surveillance and CCTV systems will always justify its means.

45.6 If the use of a surveillance and CCTV system is too privacy intrusive, the school will seek alternative provision.

46. Code of practice

46.1 The school understands that recording images of identifiable individuals constitutes as processing personal information, so it is done in line with data protection principles.

46.2 The school notifies all pupils, staff and visitors of the purpose for collecting surveillance data via signs in the school grounds where cameras are based.

46.3 CCTV cameras are only placed where they do not intrude on anyone's privacy and are necessary to fulfil their purpose.

46.4 All surveillance footage will be kept for a maximum of one month depending on the volume of recording for security purposes..

46.5 The surveillance and CCTV system is owned by the school and images from the system are strictly controlled and monitored by authorised personnel only.

46.6 The school will ensure that the surveillance and CCTV system is used to create a safer environment for staff, pupils and visitors to the school, and to ensure that its operation is consistent with the obligations outlined in data protection legislation.

47. Access

47.1 Under the GDPR, individuals have the right to obtain confirmation that their personal information is being processed as detailed in Section 14

47.2 All disks containing images belong to, and remain the property of, the school.

47.3 If appropriate a copy of the information will be supplied to the individual free of charge; however, the school may impose a 'reasonable fee' to comply with requests for further copies of the same information.

47.4 Releasing the recorded images to third parties will be permitted only in the following limited and prescribed circumstances, and to the extent required or permitted by law:

i) The police – where the images recorded would assist in a specific criminal inquiry

ii) Prosecution agencies – such as the Crown Prosecution Service (CPS)

iii) Relevant legal representatives – such as lawyers and barristers

iv) Persons who have been recorded and whose images have been retained where disclosure is required by virtue of Data Protection Legislation and the Freedom of Information Act 2000

The school's Data Protection Officer is:

John Person, john.pearson-hicks@london.anglican.org