ST PAUL'S SCHOOL

Est. 1509

Data Protection Policy

Author/reviewer responsible:	COO	ISI DOC CODE:	n/a
Reviewed by:	Op Exec	Date of last review:	05/18
Authorised by resolution of:	Governing Body	Date of authorisation:	06/18
Applicable	SPJ & SPS	Date of next review:	Under Review as of September 19

This policy is available on the Handbook page of the School Intranet and policies page of the School website and can be made available in large print or other accessible format if required; such requests can be made by email to the Chief Operating Officer: OpsDir@stpaulsschool.org.uk.

Contents

1. References

1.1 Legal and regulatory framework:

- General Data Protection Regulation (EU 2016/679)
- The UK Data Protection Act 2018 (to follow)
- The Privacy and Electronic Communications Regulations 2011
- The Protection of Freedoms Act 2012
- Guide to the General Data Protection Regulation – Information Commissioner's Office

1.2 Relevant School Policies:

- St Paul's and St Paul's Juniors Codes of Conduct
- eSafety Policy

2. General Principles

2.1 The General Data Protection Regulation (GDPR) is a European Commission Regulation intended to strengthen and unify data protection for individuals within the European Union (EU). The Commission's primary objectives of the GDPR are "to give citizens back the control of their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU". The EU Council and the Parliament both adopted the regulation in April 2016. The regulation is effective from 25 May 2018. On 14 September 2017, the UK Data Protection Bill was published. This will replace the Data Protection Act (DPA) 1998 and incorporate the GDPR into UK legislation. The DPA does not replace or contradict GDPR: rather, it is expected to bring it into UK law at the same start date as the GDPR.

2.2 **Core Principles**. The GDPR eight core principles (fairness, lawfulness and transparency; purpose limitation; data minimisation; data quality; security; integrity and confidentiality) and cross border transfer remain largely unchanged from the previous Data Protection Act.

2.2.1 St Paul's and St Paul's Juniors process large amounts of "personal data" about members of the school community. Under the GDPR and DPA, the school must process such personal data "fairly". This includes telling pupils and parents how their personal data will be held and used by the school. This data protection policy is intended to help meet that legal requirement. It should be noted, from the outset, that data protection should always take second place to safeguarding and child protection. If there is a potential conflict between the 2 competing requirements, the welfare of the child is paramount.

2.3 **This Policy**

2.3.1 This policy is intended to provide information on the school's use of personal data about individuals including current, past and prospective pupils; and their parents, carers or guardians (referred to in this policy as "parents"), staff and visitors. It should be read in conjunction with the school's Privacy Notices (of which there are 4: a general one for the school, one specifically for the staff, one specifically for pupils over 13 years of age and one for the Old Pauline Club). It applies in addition to the school's terms and conditions, and any other information the school may provide about a particular use of personal data.

2.3.2 Anyone who works for, or acts on behalf of, the school (including staff, volunteers, governors and service providers) should also be aware of and comply with this data protection policy, as well as the Privacy Notices.

2.4 **Responsibility for Data Protection**

2.4.1 In accordance with the UK DPA and GDPR, the school has notified the Information Commissioner's Office of its processing activities. The school's ICO registration number is Z7315216 and its registered address is ST PAUL'S SCHOOL, LONSDALE ROAD, LONDON, SW13 9JT.

2.4.2 Whilst St Paul's School is the Data Controller for the school and St Paul's Juniors, the School has appointed the Chief Operating Officer as Data Protection Officer ("DPO") who will

endeavour to ensure that all personal data is processed in compliance with this policy and the Act.

2.5 **The Principles of the DPA**

2.5.1 Everyone responsible for using data has to follow strict rules called 'data protection principles'. They must make sure the information is:

- Personal data shall be processed fairly and lawfully.
- Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
- Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
- Personal data shall be accurate and, where necessary, kept up to date.
- Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
- Personal data shall be processed in accordance with the rights of data subjects under this Act.
- Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
- Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

2.6 **Types of Personal Data Processed by the School**

2.6.1 The school may process a wide range of personal data about individuals including staff, current, past and prospective pupils and their parents as part of its operation, including by way of example:

- names, addresses, telephone numbers, e-mail addresses and other contact details;
- car details (about those who use our car parking facilities);
- bank details and other financial information, e.g. about parents who pay fees to the school;
- past, present and prospective pupils' academic, disciplinary, admissions and attendance records (including information about any special needs), and examination scripts and marks;
- personnel files, including in connection with academics, employment or safeguarding;

- where appropriate, information about individuals' health and welfare, and contact details for their next of kin;
- references given or received by the school about pupils, and relevant information provided by previous educational establishments and/or other professionals or organisations working with pupils;
- correspondence with and concerning staff, pupils and parents past and present; and
- images of pupils (and occasionally other individuals) engaging in school activities, and images captured by the school's CCTV system (in accordance with the school's policy on taking, storing and using images of children);

2.6.2 Generally, the school receives personal data from the individual directly (or, in the case of pupils, from parents). However, in some cases personal data may be supplied by third parties (for example another school, or other professionals or authorities working with that individual), or collected from publicly available resources.

2.7 **Special Category Data**

2.7.1 In addition, the school will on occasion need to process **special category personal data** (concerning health, ethnicity, religion, biometrics or sexual life) or criminal records information (such as when carrying out DBS checks) in accordance with rights or duties imposed on it by law, including as regards safeguarding and employment, or from time to time by explicit consent where required. Further details can be found in the applicable Privacy Notice.

2.8 **Data Accuracy and Security**

2.8.1 The school will endeavour to ensure that all personal data held in relation to an individual is as up to date and accurate as possible. Individuals must notify the DPO of any changes to information held about them. An individual has the right to request that inaccurate information about them is erased or corrected (subject to certain exemptions and limitations under the Act) and may do so by contacting the DPO in writing. The school will take appropriate technical and organisational steps to ensure the security of personal data about individuals, ensuring that it is held in accordance with the Principles of the DPA and GDPR. All staff will be made aware of this policy and their duties under the DPA.

2.9 Safeguarding Practice and Information Sharing

2.9.1 Whilst the DPA and GDPR place duties on organisations and individuals to process personal information fairly and lawfully, it is not a barrier to sharing information where the failure to do so would result in a child or vulnerable adult being placed at risk of harm. Similarly, human rights concerns, such as respecting the right to a private and family life would not prevent sharing where there are real safeguarding concerns. The Local Safeguarding Children Board (LSCB) can require an individual or body to comply with a request for information, as outlined in the Children and Families Act 2014. This can only take place when the information requested is for the purpose of enabling or assisting the LSCB to perform its functions. Any

request for information about individuals should be necessary and proportionate to the reason for the request and should be made to Designated Safeguarding Leads or Safeguarding Coordinator who must discuss any such request with the Data Protection Officer.

2.10 Rights of Access to Personal Data ("Subject Access Request")

2.10.1 The GDPR and Act provide for a right enjoyed by all individuals to know what personal data about them is being held and used by organisations (including schools), and broadly for what purpose, where it came from, and who else might receive it. This is subject to certain limitations and exemptions. Any individual wishing to access their personal data should put their request in writing to the DPO. There is no specific format for this. The school will endeavour to respond to any such written requests (known as "subject access requests") as soon as is reasonably practicable and in any event within statutory time-limits: the GDPR (SAR) requires a response within a calendar month, starting with the date on which the SAR is received (or the date on which the information referred to above is received, if later – though this should not be used to artificially extend the deadline).

2.10.2 **Fees.** The School does not charge for complying with a request unless the request is 'manifestly unfounded or excessive'. The school may charge a reasonable administrative fee if further copies are requested. If a request is 'manifestly unfounded or excessive', the school can charge a fee or refuse to respond but will provide evidence of how the conclusion that the request is manifestly unfounded or excessive was reached.

2.10.3 **Personal Data.** A SAR only provides access to the individual's own "personal data". Case law suggests that this is widely defined to include anything that "relates to" an identifiable, living individual (which means it includes initials, nicknames, job titles and so on). All the same, it is worth remembering that the right only relates to personal data, not whole documents. Where personal data about the person making a SAR also constitutes "personal data" about another person (a "third party"), a data controller is not obliged to disclose this mixed data in response to a SAR unless either (a) the third party has consented or (b) it is "reasonable", taking into account all the relevant circumstances, to disclose without consent. Otherwise, factors will include the third party's views, any harm or distress that may come to them, and their expectations of confidentiality – but the data controller must disclose as much of the requester's personal data as they can without unreasonably identifying the third party. The School is aware that it will always be assumed reasonable to disclose where that other person is a social worker or education worker, which latter definition will include from 25 May 2018 teachers (and other staff) of an independent school.

2.10.4 **Exemptions.** All members of the school community should be aware that certain data is exempt from the right of access under the Act. For example, information may be exempt from disclosure if it:

- is *legally privileged* (but this is not always easy to argue in quasi-legal processes like school complaints;
- records the intentions of the school in *negotiations* with the individual making the SAR;
- consists of a *confidential reference* given by the school (though not currently confidential references received by the school – although this wording is more ambiguous under the draft DPA 2018);

- consists of *exam or test answers* or *exam results* before the allotted publication time;
- is held for purposes of *management planning* (e.g. redundancy planning);
- would prejudice the prevention and detection of *crime* if disclosed (e.g. in live investigations);
- might cause serious harm or distress in limited *social work* contexts.

3. Data Protection for Staff

3.1 The aim of this section is to detail how the data protection policy might affect pupils and parents of St Paul's School and St Paul's Juniors and should be read in conjunction with Section 2, General Principles.

3.2 **The Data Protection Code of Conduct**

3.2.1 The following Code must be adhered to at all times:

- Staff should only ever share information on a "need to know basis".
- Data protection should never be used as an excuse for not sharing information where necessary. The welfare of the child is paramount.
- Seniority does not give an automatic right to information.
- All emails are disclosable, less a few exemptions.
- Only keep data for as long as is necessary.
- Report Data Breaches Immediately.

3.3 Confidentiality

3.3.1 Any School information/records including details of pupils, parents and employees whether actual, potential or past, other than those contained in authorised and publicly available documents, must be kept confidential unless the School's prior written consent has been obtained. This requirement exists both during and after employment. In particular, such information for the benefit of any future employer.

3.3.2 The law states that where a teacher is facing an allegation of a criminal offence involving a pupil registered at the School, the teacher concerned is entitled to anonymity until the teacher is either charged with an offence or the anonymity is waived by the teacher. If publication is made on behalf of the School, the School, including senior management and governors could be prosecuted. If a teacher is charged with such an offence, all communication must be directed through the High Master, Surmaster or Head who will have authority to deal with the allegation and any enquiries to ensure that this restriction is not breached. If a member of staff is found to have breached (whether intentionally or otherwise) this duty, any accusations will be dealt with under the School's Disciplinary Procedure.

3.4 Off Site Access

3.4.1 See also the School's eSafety Policy which states that: "The School must ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data. This is in

relation to data belonging to all members of the school community. As such, no member of staff is permitted to remove Special Category personal data (as defined in Section 2 of this Data Protection Policy) from School premises, whether in paper or electronic form and wherever stored, without prior consent of the High Master, Surmaster, Head or Chief Operating Officer (for support staff) (see the exclusions at 3.4.2 below). Where a member of staff is permitted to download data off site it will need to be password protected. The IT Support Cell can give advice and assistance, and the following are the most basic precautions for personal IT that should be put in place by all members of staff:

- Back up data – know where, how, when and what is being backed up.
- Install and turn on anti-malware software.
- Ensure you are aware where your USB drives (and memory cards) are located. Encrypt if they contain personal information.
- Switch on your firewall.
- Mobile devices – switch on password protection, keep the device up to date.
- Make sure lost or stolen devices can be tracked, locked or wiped.
- Do not connect to wi-fi hotspots.

3.4.2 There are two exceptions where prior approval is not required:

- iSAMS, the School's data management system, may be used on personal devices provided that the device is secure and password protected.
- For pupils on residential trips, medical information and other relevant information (e.g. passport details) may be taken off site by the trip leader.

4. Taking, Storing and Using Images of Children

4.1 This section is intended to provide information to pupils and their parents, carers or guardians (referred to in this policy as "parents") about how images of pupils are normally used by St Paul's School ("the school"). It also covers the school's approach to the use of cameras and filming equipment at school events and on school premises by parents and pupils themselves, and the media. It applies in addition to the school's parent contract, and any other information the school may provide about a particular use of pupil images, including e.g. signage about the use of CCTV; and more general information about use of pupils' personal data, e.g. the school's Privacy Notice.

4.2 General Points.

4.2.1 Certain uses of images are necessary for the ordinary running of the school; other uses are in the legitimate interests of the school and its community and unlikely to cause any negative impact on children. The school is entitled lawfully to process such images and take decisions about how to use them, subject to any reasonable objections raised.

4.2.2 Parents who accept a place for their child at the school are invited to agree to the school using images of him as set out in this policy. However, parents should be aware of the fact that certain uses of their child's images may be necessary or unavoidable (for example if they are included incidentally in CCTV or a photograph).

4.2.3 We hope parents will feel able to support the school in using pupil images to celebrate the achievements of pupils, sporting and academic; to promote the work of the school; and for important administrative purposes such as identification and security.

4.2.4 Any parent who wishes to limit the use of images of a pupil for whom they are responsible should contact the Chief Operating Officer, as the Data Protection Officer in writing. The School will respect the wishes of parents/carers (and indeed pupils themselves) wherever reasonably possible, and in accordance with this policy.

4.2.5 Parents should be aware that, from around the age of 12 and upwards, the law recognises pupils' own rights to have a say in how their personal information is used – including images.

4.3 **Use of Pupil Images in School Publications**

4.3.1 Unless the relevant pupil or his or her parent has requested otherwise, the school will use images of its pupils to keep the school community updated on the activities of the school, and for marketing and promotional purposes, including:

4.3.2 on internal displays (including clips of moving images) on digital and conventional notice boards within the school premises;

4.3.3 in communications with the school community (parents, pupils, staff, Governors and alumni) including by email, on the school intranet and by post;

4.3.4 on the school's website and, where appropriate, via the school's social media channels, e.g. Twitter, Instagram and Facebook. Such images would not normally be accompanied by the pupil's full name without permission; and

4.3.5 in the school's prospectus, and in online, press and other external advertisements for the school. Such external advertising would not normally include pupil's names [and in some circumstances the school will seek the parent or pupil's specific consent, depending on the nature of the image or the use].

4.3.6 The source of these images will predominantly be the school's staff (who are subject to policies and rules in how and when to take such images), or a professional photographer used for marketing and promotional purposes, or occasionally pupils. The school will only use images of pupils in suitable dress [and the images will be stored securely and centrally].

4.4 **Use of Pupil Images for Identification and Security**

4.4.1 All pupils are photographed on entering the school and, thereafter, at intervals, for the purposes of internal identification. These photographs identify the pupil by name, year group, house and form/tutor group.

4.4.2 CCTV is in use on school premises, and will sometimes capture images of pupils. Images captured on the School's CCTV system are used in accordance with the Privacy Notice and CCTV

Policy / any other information or policies concerning CCTV which may be published by the school from time to time.

4.5 **Use of Pupil Images in the Media**

4.5.1 Where practicably possible, the school will always notify parents in advance when the media is expected to attend an event or school activity in which school pupils are participating, and will make every reasonable effort to ensure that any pupil whose parent or carer has refused permission for images of that pupil, or themselves, to be made in these circumstances are not photographed or filmed by the media, nor such images provided for media purposes.

4.5.2 The media often asks for the names of the relevant pupils to go alongside the images, and these will be provided where parents have been informed about the media's visit and either parent or pupil has consented as appropriate.

4.6 **Security of Pupil Images**

4.6.1 Professional photographers and the media are accompanied at all times by a member of staff when on school premises. The school uses only reputable professional photographers and makes every effort to ensure that any images of pupils are held by them securely, responsibly and in accordance with the school's instructions.

4.6.2 The school takes appropriate technical and organisational security measures to ensure that images of pupils held by the school are kept securely on school systems, and protected from loss or misuse. The school will take reasonable steps to ensure that members of staff only have access to images of pupils held by the school where it is necessary for them to do so.

4.6.3 All staff are given guidance on the school's Policy on Taking, Storing and Using Images of Pupils, and on the importance of ensuring that images of pupils are made and used responsibly, only for school purposes, and in accordance with school policies and the law.

4.7 **Use of Cameras and Filming Equipment (including mobile phones) by Parents**

4.7.1 Parents, guardians or close family members (hereafter, parents) are welcome to take photographs of (and where appropriate, film) their own children taking part in school events, subject to the following guidelines, which the school expects all parents to follow:

4.7.2 When an event is held indoors, such as a play or a concert, parents should be mindful of the need to use their cameras and filming devices with consideration and courtesy for cast members or performers on stage and the comfort of others. Flash photography can disturb others in the audience, or even cause distress for those with medical conditions; the school therefore asks that it is not used at indoor events.

4.7.3 Parents are asked not to take photographs of other pupils, except incidentally as part of a group shot, without the prior agreement of that pupil's parents.

4.7.4 Parents are reminded that such images are for personal use only. Images which may, expressly or not, identify other pupils should not be made accessible to others via the internet (for example on Facebook), or published in any other way.

4.7.5 Parents are reminded that copyright issues may prevent the school from permitting the filming or recording of some plays and concerts. The school will always print a reminder in the programme of events where issues of copyright apply.

4.7.6 Parents may not film or take photographs in changing rooms or backstage during school productions, nor in any other circumstances in which photography or filming may embarrass or upset pupils.

4.7.7 The school reserves the right to refuse or withdraw permission to film or take photographs (at a specific event or more generally), from any parent who does not follow these guidelines, or is otherwise reasonably felt to be making inappropriate images.

4.7.8 The school sometimes records plays and concerts professionally (or engages a professional photographer or film company to do so), in which case CD, DVD or digital copies may be made available to parents for purchase. Parents of pupils taking part in such plays and concerts will be consulted if it is intended to make such recordings available more widely.

4.8 **Use of Cameras and Filming Equipment by Pupils**

4.8.1 All pupils are encouraged to look after each other, and to report any concerns about the misuse of technology, or any worrying issues to a member of the pastoral staff.

4.8.2 The use of cameras or filming equipment (including on mobile phones) is not allowed in toilets, washing or changing areas, nor should photography or filming equipment be used by pupils in a manner that may offend or cause upset.

4.8.3 The misuse of images, cameras or filming equipment in a way that breaches this Policy, or the school's Anti-Bullying Policy, Data Protection Policy for Pupils, Parents and Carers, eSafety Policy, IT Acceptable Use Policy for Pupils, Safeguarding Policy or the School Rules is always taken seriously, and may be the subject of disciplinary procedures or dealt with under the relevant safeguarding policy as appropriate.

5 Data Breaches

5.1.1 **What is a 'personal data breach'?** A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable and this unavailability has a significant negative effect on individuals. A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

3.6.2 Personal data breaches can include:

- access by an unauthorised third party;
- deliberate or accidental action (or inaction) by a controller or processor;

- sending personal data to an incorrect recipient;
- computing devices containing personal data being lost or stolen;
- alteration of personal data without permission; and
- loss of availability of personal data.

They should be reported to the Information Commissioner's Office by the DPO if the breach will result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage.

3.6.2 In the event of a breach, the member of staff must notify the Data Protection Officer within 24 hours of becoming aware of the breach. This notification must include at least:

- your name and contact details;
- the date and time of the breach (or an estimate);
- the date and time you detected it;
- basic information about the type of breach; and
- basic information about the personal data concerned.

3.6.3 The DPO will then make a judgement on the best course of action which is likely to include notifying the High Master, Surmaster and/or Head, plus the Designated Safeguarding Lead in the event that the data breach includes pupils' details, as appropriate. The DPO will then report the breach, if required, ""…*without undue delay and, where feasible, not later than 72 hours after having become aware of it… <u>unless</u> the breach is unlikely to result in a risk to the rights and freedoms of natural persons*."

STEP GUIDE TO DATA BREACH RESPONSE

1. Upon the first employee becoming aware of the breach

    - *Am I the relevant person at the organisation? If not, immediately notify that person – this should be the DPO.*

2. Initial assessment, containment and recovery – first few hours:

    - *How long has the breach been active, what data was involved and how far has it got?*
    - *What immediate steps can be taken to prevent it going further? Consider:*
        - *if a cyber breach, involve the school's IT personnel from the outset;*
        - *if human actor(s) are involved, can they be contacted to give reassurances;*
        - *if e.g. Royal Mail, courier, IT or other contractors are involved, can they assist;*
        - *are specialists needed: forensic IT consultants, crisis management PR, legal etc.*

3. Ongoing assessment of risk and mitigation – first 72 hours (and initial notification where required):

- *Build up a more detailed picture of the risk and reach of the security breach:*
  - *how many have been affected?*
  - *was any sensitive personal data involved – health, sexual life, crime?*
  - *was financial data involved and/or is there a risk of identify fraud?*
- *Identify if a crime has been committed and involve police or cyber fraud unit.*
- *Assess if insurers need notifying (major loss, crime, or possible legal claim(s))*
- *Decide if the likely risk of harm to the data subjects:*
  - *is sufficient to require a full or preliminary notification to the ICO; and*
  - *is sufficiently serious to require communication to affected individuals*
- *If not, is this a matter we can document but deal with internally?; or*
- *If so, what can we usefully tell the ICO and/or individuals at this stage?*
  - *e.g. provide fraud or password advice, offer counselling etc.*

4. Ongoing evaluation, monitoring and remediation:

- *Continue to monitor and assess possible consequences (even if apparently contained).*
- *Keep the ICO and/or those affected informed as new information becomes available.*
- *Tell the ICO and/or those affected what you are doing to remediate and improve practice.*
- *Begin process of review internally:*
  - *how did this happen? What could we have done better?*
  - *would training or even disciplinary action be justified for staff members?*
  - *were our policies adequate, and/or adequately followed?*
  - *if our contractors were involved (e.g. systems providers), did they respond adequately? Do we have any remedies against them if not?*

5. Record keeping and putting outcomes into practice:

- *Keep a full internal record, whether or not the matter was reported or resulted in harm.*
- *Log this record against wider trends and compare with past incidents.*
- *Make sure all past outcomes were in fact put into practice.*
- *Ensure any recommendations made by, or promised to, the ICO are actioned.*
- *Notify the Charity Commission as an RSI, if a charity, at an appropriate juncture.*
- *Review policies and ensure regular (or specific, if required) training is actually completed.*

Serious breaches should be reported to the ICO using the security breach helpline on 0303 123 1113 (open Monday to Friday, 9am to 5pm). Select option 3 to speak to staff who will record the breach and give advice. The security breach notification form can be found here.

6. Data Protection for Pupils

6.1 The aim of this section is to detail how the data protection policy might affect pupils at St Paul's School and St Paul's Juniors and should be read in conjunction with Section 2, General Principles.

6.2 **Subject Access Requests**

6.2.1 In addition to the general principles outlined in Section 2:

- Pupils can make subject access requests for their own personal data, provided that, in the reasonable opinion of the school, they have sufficient maturity to understand the request they are making. Pupils aged 13 or over are generally assumed to have this level of maturity, although this will depend on both the child and the personal data requested. All subject access requests from pupils will therefore be considered on a case by case basis.

- **Third Party Requests**. The school will respond to SARs from a third party provided that it is satisfied that the third party is genuinely acting on the individual's behalf – for example, by their solicitor, or a family member. Children have exactly the same rights to make a SAR as adults. Strictly speaking those rights belong to the child (and not the parent). However, a person with parental responsibility would normally exercise those rights on behalf of a child too young to understand the nature of the request (usually meaning under 12). A child of any age can also ask a parent or third party to make a SAR on their behalf.

6.2.2 Pupils are required to respect the personal data and privacy of others, and to comply with the school's IT Acceptable Use Policy and the school rules.

6.3 **Queries and Complaints**

6.3.1 Any comments or queries on this policy should be directed to the DPO using the following contact details: Edward Flute, Chief Operating Officer, St Paul's School, Lonsdale Road, Barnes, SW13 9JT.

6.3.2 If an individual believes that the school has not complied with this policy or acted otherwise than in accordance with the Act, they should utilise the school complaints/grievance procedure and should also notify the DPO.

7. Data Retention and Storage Guidelines

7.5.1 In these guidelines, "record" means any document or item of data which contains evidence or information relating to the school, its staff or pupils. Some of this material, but not all, will contain personal data of individuals as defined in the DPA. An obvious example of personal data would be the Single Central Record or a pupil file; however, a "record" of personal data could arise simply by holding an email on the school's systems. Many, if not most, new and recent records will be created, received and stored electronically. Others (such as Certificates, Registers, or older records) will be original paper documents. The format of the record is less important than its contents and the purpose for keeping it.

7.5.2 Storage of Records

Records should be stored as follows:

7.2.1 **Digital records.** Digital records can be lost or misappropriated in huge quantities very quickly. Access to sensitive data – or any large quantity of data – is, as a minimum, password-protected and held on a limited number of devices only, with passwords provided on a need-to-know basis and regularly changed. Where 'cloud storage' is used, data needs have to be considered. If personal information kept in this way is sensitive, or held in large quantities, digital encryption is to be used. Emails (whether they are retained electronically or printed out as part of a paper file) are also "records" and may be particularly important: whether as disclosable documents in any litigation, or as representing personal data of the sender (or subject) for data protection/data privacy purposes. Again, however, the format is secondary to the content and the purpose of keeping the document as a record. It is also worth remembering that a digital document's original metadata may indicate the date of its creation, its author or the history of its changes: so it is important that this information is preserved.

7.2.2 **Paper records**. Paper records are most often damaged by damp or poor storage conditions; the school ensures that all paper files are stored in dry, cool storage with appropriate security measures in place. Under the DPA, paper records are only classed as personal data if held in a "relevant filing system". This means organised, and/or indexed, such that specific categories of personal information relating to a certain individual are readily accessible, and thus searchable as a digital database might be. By way of example, an alphabetical personnel file split into marked dividers will likely fall under this category: but a merely chronological file of correspondence may well not. However, when personal information is contained on print-outs taken from electronic files, this data has already been processed by the school and falls under the DPA.

7.3 **Archiving and the Destruction or Erasure of Records.**

7.3.1 All staff receive basic training in data management – issues such as security, recognising and handling sensitive personal data, safeguarding etc. Staff given specific responsibility for the management of records have specific training and ensure, as a minimum, the following:

- That records – whether electronic or hard copy – are stored securely as above, including if possible with encryption, so that access is available only to authorised persons and the records themselves are available when required and (where necessary) searchable;

- That important records, and large or sensitive personal databases, are not taken home or – in respect of digital data – carried or kept on portable devices (whether CDs or data sticks, or mobiles and handheld electronic tablets) unless absolutely necessary, in which case it should be subject to a risk assessment and in line with the school's e-Safety policy;

- That back ups are made only by the IT Support Cell and not individual ad hoc action;

- That arrangements with external storage providers – whether physical or electronic (in any form, but most particularly "cloud-based" storage) – are supported by robust contractual arrangements (Data Processing Agreements) providing for security and access;

- That reviews are conducted on a regular basis, in line with the guidance below, to ensure that all information being kept is still relevant and – in the case of personal data – necessary for the purposes for which it is held (and if so, that it is accurate and up-to-date); and

- That all destruction or permanent erasure of records, if undertaken by a third party, is carried out securely – with no risk of the re-use or disclosure, or re-construction, of any records or information contained in them.

7.4 **Table of Suggested Retention Periods**

Type of Record/Document	**<u>Suggested</u> Retention Period**
<u>SCHOOL-SPECIFIC RECORDS</u>	
• Registration documents of School	Permanent (or until closure of the school)
• Attendance Register	6 years from last date of entry, then archive.
• Minutes of Governors' meetings	Minimum 6 years from date of meeting
• Annual curriculum	From end of year: 3 years (or 1 year for other class records: eg marks / timetables / assignments)
<u>INDIVIDUAL PUPIL RECORDS</u>	***NB – this will generally be personal data***
• Admissions: application forms, assessments, records of decisions	25 years from date of birth (or, if pupil not admitted, up to 7 years from that decision).
• Examination results (external or internal)	7 years from pupil leaving school
• Pupil file including: o Pupil reports o Pupil performance records o Pupil medical records	ALL: 25 years from date of birth (subject to where relevant to safeguarding considerations: any material which may be relevant to potential claims should be kept for the lifetime of the pupil).
• Special educational needs records (*to be risk assessed individually*)	Date of birth plus up to 35 years (allowing for special extensions to statutory limitation period)
<u>SAFEGUARDING</u>	
• Policies and procedures	Keep a permanent record of historic policies
• DBS disclosure certificates (if held)	<u>No longer than 6 months</u> from decision on recruitment, unless DBS specifically consulted – but a record of the checks being made must be kept, if not the certificate itself.
• Accident / Incident reporting	Keep on record for as long as any living victim may bring a claim (NB civil claim limitation periods can

Type of Record/Document	Suggested Retention Period
• Child Protection files	be set aside in cases of abuse). Ideally, files to be reviewed from time to time if resources allow and a suitably qualified person is available. [2] If a referral has been made / social care have been involved or child has been subject of a multi-agency plan – indefinitely. If low level concerns, with no multi-agency act – apply applicable school low-level concerns policy rationale (this may be 25 years from date of birth OR indefinitely).
CORPORATE RECORDS (where applicable) • Certificates of Incorporation • Minutes, Notes and Resolutions of Boards or Management Meetings • Register of Members/Shareholders • Annual reports	 Permanent (or until dissolution of the company) Minimum – 10 years Permanent (minimum 10 years for ex-members/shareholders) Minimum – 6 years
ACCOUNTING RECORDS • Accounting records (*normally taken to mean records which enable a company's accurate financial position to be ascertained & which give a true and fair view of the company's financial state*) • Tax returns • VAT returns • Budget and internal financial reports	 Minimum – 6 years for private UK companies (except where still necessary for tax returns) Minimum – 6 years for UK charities (and public companies) from the end of the financial year in which the transaction took place Internationally: can be up to 20 years depending on local legal/accountancy requirements Minimum – 6 years Minimum – 6 years Minimum – 6 years

Type of Record/Document	Suggested Retention Period
CONTRACTS AND AGREEMENTS	
• Signed or final/concluded agreements (*plus any signed or final/concluded variations or amendments*)	Minimum – 7 years from completion of contractual obligations or term of agreement, whichever is the later
• Deeds (or contracts under seal)	Minimum – 13 years from completion of contractual obligation or term of agreement
INTELLECTUAL PROPERTY RECORDS	
• Formal documents of title (trade mark or registered design certificates; patent or utility model certificates)	Permanent (in the case of any right which can be permanently extended, eg trademarks); otherwise expiry of right plus minimum of 7 years.
• Assignments of intellectual property to or from the school	As above in relation to contracts (7 years) or, where applicable, deeds (13 years).
• IP / IT agreements (including software licences and ancillary agreements eg maintenance; storage; development; coexistence agreements; consents)	Minimum – 7 years from completion of contractual obligation concerned or term of agreement
EMPLOYEE / PERSONNEL RECORDS	***NB this will contain personal data***
• Single Central Record of employees	Keep a permanent record of all mandatory checks that have been undertaken (but not DBS certificate itself: 6 months as above)
• Contracts of employment	Minimum 7 years from effective date of end of contract
• Employee appraisals or reviews	Duration of employment plus minimum of 7 years
• Staff personnel file	As above, but do not delete any information which may be relevant to historic safeguarding claims.
• Payroll, salary, maternity pay records	Minimum – 6 years
• Pension or other benefit schedule records	Possibly permanent, depending on nature of scheme
• Job application and interview/rejection records (unsuccessful applicants)	Minimum 3 months but no more than 1 year
• Immigration records	Minimum – 4 years

Type of Record/Document	Suggested Retention Period
• Health records relating to employees	7 years from end of contract of employment
INSURANCE RECORDS • Insurance policies (will vary – private, public, professional indemnity) • Correspondence related to claims/ renewals/ notification re: insurance	Duration of policy (or as required by policy) plus a period for any run-off arrangement and coverage of insured risks: ideally, until it is possible to calculate that no living person could make a claim. Minimum – 7 years
ENVIRONMENTAL, HEALTH & DATA • Maintenance logs • Accidents to children • Accident at work records (staff) • Staff use of hazardous substances	10 years from date of last entry 25 years from birth (longer for safeguarding) Minimum – 4 years from date of accident, but review case-by-case where possible Minimum – 7 years from end of date of use
• Risk assessments (carried out in respect of above) • Data protection records documenting processing activity, data breaches	7 years from completion of relevant project, incident, event or activity. No limit: as long as up-to-date and relevant (as long as no personal data held)

8. CCTV Policy

8.1 The purpose of this policy is to regulate the management and operation of the Closed Circuit Television (CCTV) System at St Paul's School (the **School**). It also serves as a notice and a guide to data subjects (including pupils, parents, staff, volunteers, visitors to the School and members of the public) regarding their rights in relation to personal data recorded via the CCTV system (the **System**).

8.1.1 The System is administered and managed by the School, who act as the Data Controller. This policy will be subject to review from time to time, and should be read with reference to the School's Data Protection Policy, which is detailed above. For further guidance, please review the Information Commissioner's CCTV Code of Practice.

8.1.2 All fixed cameras are in plain sight on the School premises and the School does not routinely use CCTV for covert monitoring or monitoring of private property outside the School grounds. The

School's purposes of using the CCTV system are set out below and, having fully considered the privacy rights of individuals, the School believes these purposes are all in its legitimate interests. Data captured for the purposes below will not be used for any commercial purpose.

8.2 **Objectives of the System**

8.2.1 The Objectives of the CCTV system are:

- To protect pupils, staff, volunteers, visitors and members of the public with regard to their personal safety.
- To protect the School buildings and equipment, and the personal property of pupils, staff, volunteers, visitors and members of the public.
- To support the police and community in preventing and detecting crime, and assist in the identification and apprehension of offenders.
- To monitor the security and integrity of the School site and deliveries and arrivals.
- To monitor staff and contractors when carrying out work duties.
- To monitor and uphold discipline among pupils in line with the [School Rules], which are available to parents and pupils on request.

8.3 **Positioning**

8.3.1 Locations have been selected, both inside and out, that the School reasonably believes require monitoring to address the stated objectives. Adequate signage has been placed in prominent positions to inform staff and pupils that they are entering a monitored area, identifying the School as the Data Controller and giving contact details for further information regarding the system.

8.3.2 No images will be captured from areas in which individuals would have a heightened expectation of privacy, including changing and washroom facilities. No images of public spaces will be captured except to a limited extent at site entrances.

8.4 **Maintenance**

8.4.1 The CCTV System will be operational 24 hours a day, every day of the year. The System Manager (defined below) will check and confirm that the System is properly recording and that cameras are functioning correctly, on a regular basis.

8.4.2 The System will be checked and (to the extent necessary) serviced no less than annually.

8.5 **Supervision of the System**

8.5.1 Staff authorised by the School to conduct routine supervision of the System may include Porters, the Receptionist, day or night security, the Estates, IT and Facilities Managers, the DPO, and relevant staff on duty.

8.5.2 Images will be viewed and/or monitored in a suitably secure and private area to minimise the likelihood of or opportunity for access to unauthorised persons.

8.6 **Storage of Data**

8.6.1 The day-to-day management of images will be the responsibility of the Head Porter who will act as the System Manager, or such suitable person as the System Manager shall appoint in his absence.

8.6.2 Images will be stored for 2 weeks, and automatically over-written unless the School considers it reasonably necessary for the pursuit of the objectives outlined above, or if lawfully required by an appropriate third party such as the police or local authority.

8.6.3 Where such data is retained, it will be retained in accordance with the Act and our Data Protection Policy. Information including the date, time and length of the recording, as well as the locations covered and groups or individuals recorded, will be recorded in the system log book.

8.7 **Access to Images**

8.7.1 Access to stored CCTV images will only be given to authorised persons, under the supervision of the System Manager, in pursuance of the above objectives (or if there is some other overriding and lawful reason to grant such access).

8.7.2 Individuals also have the right to access personal data the School holds on them (please see the Data Protection Policy above), including information held on the System, if it has been kept. The School will require specific details including at least to time, date and camera location before it can properly respond to any such requests. This right is subject to certain exemptions from access, including in some circumstances where others are identifiable.

8.7.3 The System Manager must satisfy themselves of the identity of any person wishing to view stored images or access the system and the legitimacy of the request. The following are examples when the System Manager may authorise access to CCTV images:

- Where required to do so by the Highmaster, Surmaster, Head, COO, the Police or some relevant statutory authority;
- To make a report regarding suspected criminal behaviour;
- To enable the Designated Safeguarding Lead or his/her appointed deputy to examine behaviour which may give rise to any reasonable safeguarding concern;
- To assist the School in establishing facts in cases of unacceptable pupil behaviour, in which case, the parents/guardian will be informed as part of the School's management of a particular incident;
- To data subjects (or their legal representatives) pursuant to an access request under the Act and on the basis set out in 6.7.2 above;
- To the School's insurance brokers where required in order to pursue a claim for damage done to insured property; or
- In any other circumstances required under law or regulation.

8.7.4 Where images are disclosed under 6.7.3 above, a record will be made in the system log book including the person viewing the images, the time of access, the reason for viewing the images, the details of images viewed and a crime incident number (if applicable).

8.8 **Other CCTV systems**

8.8.1 The School does not own or manage third party CCTV systems, but may be provided by third parties with images of incidents where this in line with the objectives of the School's own CCTV policy and/or its School Rules.

8.8.2 Many pupils travel to School on coaches provided by third party contractors and a number of these coaches are equipped with CCTV systems. The School may use these in establishing facts in cases of unacceptable pupil behaviour, in which case the parents/guardian will be informed as part of the School's management of a particular incident.

8.9 **Complaints and queries**

8.9.1 Any complaints or queries in relation to the School's CCTV system, or its use of CCTV, or requests for copies, should be referred to the DPO.

Annex:

A. Access to CCTV Image Request Form.

St Paul's School
Lonsdale Road, Barnes, SW13 9JT

ACCESS TO CCTV IMAGE REQUEST FORM

You must fill this form in if you require access to CCTV images held by St Paul's School.

SECTION ONE: YOUR DETAILS

Name:_____

Name of your company/organisation/ person you represent:_____

Position in the company/organisation:_____

SECTION TWO: WHY CCTV IMAGES ARE REQUESTED

Please tick the applicable box:

You represent the police or other law enforcement agency, and the images are required to prevent/detect a crime and/or identify, apprehend or prosecute offenders. ☐

You represent a prosecution agency and require the images to prosecute an offender. ☐

You are a solicitor or barrister and require the images in connection with legal proceedings. ☐

You represent the media, where disclosure of the image to the public is need in order to assist in the identification of a victim, witness or perpetrator in relation to the criminal incident. ☐

SECTION THREE: DETAILS OF THE CCTV IMAGE YOU WANT ACCESS TO

(1.) What is the date, location and approximate time of the images you wish to view?

_____

(2.) Please provide details of the incident and description or person, vehicle or property:

_____

(3.) Will you need to take a copy of the images away from the site? YES / NO

(4.) If yes, please give reason.

_____

SECTION FOUR: DECLARATION

I certify that I am authorised to represent the company/organisation/person listed above and the images are requested in connection with the prevention/diction of a crime, the apprehension or prosecution of offenders, criminal proceedings or public safety.

I confirm that the information I have provided on this form is true and accurate. I agree that I and the organisation/company/person I represent will only use the images in connection with the purposes for which St Paul's School has provided me. My organisation fully understands the implications of the Data Protection Act 1998. They also understand that where the images are taken off site, it will become the Data Controller in respect of the personal data contained in those CCTV images.

Signed:

Date:

Title/Position:

9. The Use of Drones

9.1 The ICO recommends that users of drones – also called unmanned aerial systems (UAS) or unmanned aerial vehicles (UAVs) – with cameras should operate them in a responsible way to respect the privacy of others. If a drone has a camera, its use has the potential to be covered by the DPA as there could be a privacy risk to other people.

9.2 **How can I use a Drone Responsibly?**

- **Let people know before you start recording**. In some scenarios this is going to be quite easy because you will know everyone within close view (for example, if you are taking a group photo at a school barbeque). In other scenarios, for example at the beach or the park, this is going to be much more difficult so you'll need to apply some common sense before you start.

- **Consider your surroundings**. If you are recording images beyond the school environs, a drone may intrude on the privacy of others where they expect their privacy to be respected (such as in their back garden).

- **Get to know your camera first**. It is a good idea to get to know the capability of your camera in a controlled situation to understand how it works. What is the quality of the image? How powerful is the zoom? Can you control when it starts and stops recording? Drone cameras are capable of taking unusual and creative pictures from original vantage points. Knowing the capabilities of your camera will help you to reduce the risk of privacy intrusion.

- **Plan your flight**. Your drone's battery life is likely to be short. By understanding its capabilities you will be able to make best use of its flight and it will be easier to plan how to avoid invading the privacy of other people. For example, it may be more privacy-friendly to launch from a different location rather than flying close to other people or their property.

- **Keep you and your drone in view**. You won't want to lose it, and if you are clearly visible then it will be easier for members of the public to know that you are the person responsible for the drone.

- **Think before sharing**. Once your drone has landed, think carefully about who's going to be looking at the images, particularly if you're thinking about posting them on social media. Avoid sharing images that could have unfair or harmful consequences. Apply the same common sense approach that you would with images or video recorded by a smartphone or digital camera.

- **Keep the images safe**. The images you have taken may be saved on an SD card or USB drive attached to the drone or the camera. If they are not necessary, then do not keep them. If you do want to keep them, then make sure they are kept in a safe place.