Data Protection Policies and Guidance

Author	Director of Operations
This Policy was approved by the Trustees*:*	Summer 2022
The implementation of this policy will be monitored by the:	Head and Director of Operations
Monitoring will take place:	Every 2 years
This Policy will be reviewed every 2 years or more regularly in the light of any significant new developments. The next anticipated review date will be:	Summer 2024

Table of Contents

Staff and Trustee Privacy Policy 2
Pupil and Parental Privacy Policy 9
Storage and Retention of Records and Documents Policy 17
Taking, Storing and Using Images of Children Policy 21
CCTV Policy 25
CCTV Footage Access Request 28
Biometric Data Policy 29
Use of Pupils' Biometric Data by the School 30
Data Breach Procedure 31
Step Guide to Data Breach Response 32
Data Protection Guidance 34
Storage and Retention of Records and Documents Guidance 35
Data Breach Guidance 44
Subject Access Request Guidance 47

Staff and Trustee Privacy Policy

This document is applicable to past and present Staff and Trustees of St Edward's School Trust Cheltenham.

In the course of your employment, engagement or other basis of work undertaken for the School, we will collect, use and hold ("process") personal data relating to you as a member of our staff. This makes the School a data controller of your personal information, and this Policy sets out how we will use that information and what your rights are.

Who this document applies to

Academic and other staff, contractors, itinerant teachers, casual workers, Trustees, temps and volunteers who may be employed or engaged by the School to work for it in any capacity, as well as prospective applicants for roles.

This policy is not aimed at pupils, or parents of pupils (whether current, past or prospective) or other members of the public, nor does it inform staff how to handle the personal data of the same.

About this document

This policy explains how the School collects, uses and shares (or "processes") personal data of staff, and your rights in relation to the personal data we hold.

This policy also applies in addition to the School's other relevant terms and conditions and policies, including:

- any contract between the School and its staff, such as the terms and conditions of employment, and any applicable staff handbook.
- the School's CCTV and/or biometrics policy;
- the School's retention of records policy;
- the School's safeguarding, pastoral, anti-bullying, or health and safety policies, including as to how concerns or incidents are reported or recorded (both by and about staff); and
- the School's IT policies, including its Acceptable Use policy and e-Safety policy.

Please note that your contract with the School, including any document or policy forming a part of your contractual obligations to the School, may in particular be relevant to and supplement the information in this policy, to the extent that it will contain details of obligations or rights of the School under contract with you which may require the use of your personal data. However, this policy is the primary document applicable to the use of your personal data by the School.

This policy also applies alongside any other information the School may provide about particular uses of personal data, for example when collecting data via an online or paper form.

Responsibility for data protection

The Bursar as Compliance Officer will deal with all your requests and enquiries concerning the School's uses of your personal data (see section on Your Rights below) and endeavour to ensure that all personal data is processed in compliance with this policy and Data Protection Law.

The School has appointed Romero Services to undertake Data Protection Officer (DPO) duties. Romero Services can be contacted by emailing dataprotection@stedwards.co.uk.

How we collect your information

We may collect your personal data in a number of ways, for example:

- from the information you provide to us before making a job application, for example when you come for an interview;
- when you submit a formal application to work for us, and provide your personal data in application forms and covering letters, etc.; and
- from third parties, for example the Disclosure and Barring Service (DBS) and referees (including your previous or current employers or School), in order to verify details about you and/or your application to work for us.

More generally, during the course of your employment with us, as a member of staff, we will collect data from or about you, including:

- when you provide or update your contact details;
- when you or another member of staff completes paperwork regarding your performance appraisals;
- in the course of fulfilling your employment (or equivalent) duties more generally, including by filling reports, note taking, or sending emails on School systems;
- in various other ways as you interact with us during your time as a member of staff, and afterwards, where relevant, for the various purposes set out below.

The types of information we collect

We may collect the following types of personal data about you (and your family members and 'next of kin', where relevant):

- contact and communications information, including:
    - your contact details (including email address(es), telephone numbers and postal address(es);
    - contact details (through various means, as above) for your family members and 'next of kin', in which case you confirm that you have the right to pass this information to us for use by us in accordance with this policy;
    - records of communications and interactions we have had with you;

- biographical, educational and social information, including:

    - your name, title, gender, nationality and date of birth;
    - your image and likeness, including as captured in photographs taken for work purposes;
    - details of your education and references from your institutions of study;
    - lifestyle information and social circumstances;
    - your interests and extra-curricular activities;

- financial information, including:

    - your bank account number(s), name(s) and sort code(s) (used for paying your salary and processing other payments);
    - your tax status (including residence status);
    - Gift Aid declaration information, where relevant (for example, where we help you to administer donations to charity from your pre-taxed earnings);
    - information related to pensions, national insurance, or employee benefit schemes;

- work related information, including:

    - details of your work history and references from your previous employer(s);
    - your personal data captured in the work product(s), notes and correspondence you create while employed by or otherwise engaged to work for the School;
    - details of your professional activities and interests;
    - your involvement with and membership of sector bodies and professional associations;
    - information about your employment and professional life after leaving the School, where relevant (for example, where you have asked us to keep in touch with you);

- and any other information relevant to your employment or other engagement to work for the School.

Where this is necessary for your employment or other engagement to work for us, we may also collect special categories of data, and information about criminal convictions and offences, including:

- information revealing your racial or ethnic origin;
- trade union membership, where applicable;
- information concerning your health and medical conditions (for example, where required to monitor and record sickness absences, dietary needs, or to make reasonable adjustments to your working conditions or environment);
- biometric information, for example where necessary for School catering, printing and security systems;
- information concerning your sexual life or orientation (for example, in the course of investigating complaints made by you or others, for example concerning discrimination); and
- information about certain criminal convictions (for example, where this is necessary for due diligence purposes, or compliance with our legal and regulatory obligations);

However, this will only be undertaken where and to the extent it is necessary for a lawful purpose in connection with your employment or other engagement to work for the School.

The bases for processing your personal data, how that data is used and whom it is shared with.

(i) Entering into, or fulfilling, our contract with you

We process your personal data because it is necessary for the performance of a contract to which you are a party or in order to take steps at your request prior to entering into a contract, such as a contract of employment or other engagement with us. In this respect, we use your personal data for the following:

- administering job applications and, where relevant, offering you a role with us;
- carrying out due diligence checks on you, whether during the application process for a role with us or during your engagement with us, including by checking references in relation to your education and your employment history;
- once you are employed or engaged by us in any capacity, for the performance of the contract of employment (or other agreement) between you and us;
- to pay you and to administer benefits (including pensions) in connection with your employment or other engagement with us;
- monitoring your attendance and your performance in your work, including in performance appraisals;
- promoting the School to prospective parents and others, including by publishing the work product(s) you create while employed by or otherwise engaged to work for the School;
- for disciplinary purposes, including conducting investigations where required;
- for other administrative purposes, for example to update you about changes to your terms and conditions of employment or engagement, or changes to your pension arrangements;
- for internal record-keeping, including the management of any staff feedback or complaints and incident reporting; and
- for any other reason or purpose set out in your employment or other contract with us.

(ii) Legitimate Interests

We process your personal data because it is necessary for our (or sometimes a third party's) legitimate interests. Our "legitimate interests" include our interests in running the School in a professional, sustainable manner, in accordance with all relevant ethical, educational, charitable, legal and regulatory duties and requirements (whether or not connected directly to data protection law). In this respect, we use your personal data for the following:

- providing you with information about us and what it is like to work for us (where you have asked for this, most obviously before you have made a formal application to work for us);
- for security purposes, including by operating security cameras in various locations on the School's premises;

- to enable relevant authorities to monitor the School's performance and to intervene or assist with incidents as appropriate;
- to provide education services to pupils;
- to safeguard pupils' welfare and provide appropriate pastoral care;
- to carry out or cooperate with any School or external complaints, disciplinary or investigatory process;
- for the purposes of management planning and forecasting, research and statistical analysis;
- in connection with organising events and social engagements for staff;
- making travel arrangements on your behalf, where required;
- contacting you or your family members and 'next of kin' for business continuity purposes, to confirm your absence from work, etc.;
- publishing your image and likeness in connection with your employment or engagement with us;
- to monitor (as appropriate) use of the School's IT and communications systems in accordance with the School's IT: acceptable use policy and government guidance such as KCSIE.

(iii) Legal Obligations

We also process your personal data for our compliance with our legal obligations, notably those in connection with employment, charity/company law, tax law and accounting, and child welfare. In this respect, we use your personal data for the following:

- to meet our legal obligations (for example, relating to child welfare, social protection, diversity, equality, and gender pay gap monitoring, employment, and health and safety);
- for tax and accounting purposes, including transferring personal data to HM Revenue and Customs to ensure that you have paid appropriate amounts of tax, and in respect of any Gift Aid claims, where relevant;
- for the prevention and detection of crime, and in order to assist with investigations (including criminal investigations) carried out by the police and other competent authorities.

(iv) Special categories of data

We process special categories of personal data (such as data concerning health, religious beliefs, racial or ethnic origin, sexual orientation or union membership) or criminal convictions and allegations for the reasons set out below.

We will process this data on the basis that such processing is necessary to carry out obligations and exercise rights (both yours and ours) in relation to your employment.

In particular, we process the following types of special category personal data for the following reasons:

- your physical or mental health or condition(s) in order to record sick leave and take decisions about your fitness for work, or (in emergencies) act on any medical needs you may have;
- recording your racial or ethnic origin in order to monitor our compliance with equal opportunities legislation;
- trade union membership, in connection with your rights as an employee and our obligations as an employer;
- categories of your personal data which are relevant to investigating complaints made by you or others, for example concerning discrimination, bullying or harassment;
- data about any criminal convictions or offences committed by you, for example when conducting criminal background checks with the DBS, or where it is necessary to record or report an allegation (including to police or other authorities, with or without reference to you);

We will process special categories of personal data for lawful reasons only, including because:

- you have given us your explicit consent to do so, in circumstances where consent is appropriate;
- it is necessary to protect your or another person's vital interests, for example, where you have a life-threatening accident or illness in the workplace and we have to process your personal data in order to ensure you receive appropriate medical attention;
- it is necessary for some function in the substantial public interest, including the safeguarding of children or vulnerable people, or as part of a process designed to protect others from malpractice, incompetence or unfitness in a role (or to establish the truth of any such allegations); or
- it is necessary for the establishment, exercise or defence of legal claims, such as where any person has brought a claim or serious complaint against us or you.

Sharing your information with others

For the purposes referred to in this policy and relying on the bases for processing as set out above, we may share your personal data with certain third parties. We may disclose limited personal data (including in limited cases special category or criminal data) to a variety of recipients including:

- other employees, agents and contractors (eg third parties processing data on our behalf as part of administering payroll services, the provision of benefits including pensions, IT etc. – although this is not sharing your data in a legal sense, as these are considered data processors on our behalf);
- DBS and other relevant authorities and agencies such as the Department for Education, NCTL, the ICO, Charity Commission and the local authority;

- external auditors or inspectors;
- our advisers where it is necessary for us to obtain their advice or assistance, including insurers, lawyers, accountants, or other external consultants;
- third parties and their advisers in the unlikely event that those third parties are acquiring or considering acquiring all or part of our School, or we are reconstituting or setting up some;
- when the School is legally required to do so (by a court order, government body, law enforcement agency or other authority of competent jurisdiction), for example HM Revenue and Customs or police.

We may also share information about you with other employers in the form of a reference, where we consider it appropriate, or if we are required to do so in compliance with our legal obligations.

How long your information is kept

Personal data relating to unsuccessful job applicants is deleted with 12 months (minimum 3 months), except where we have notified you we intend to keep it for longer (and you have not objected).

For employees, subject to any other policies that we may provide to you, we may retain your personal data for a period of 7 years after your contract of employment (or equivalent agreement) has expired or been terminated.

However, some information may be retained for longer than this, for example incident reports and safeguarding files, in accordance with specific legal requirements. Please see Storage and Retention of Records and Documents Policy.

Your rights

Your rights as a 'data subject' are the same as if you were any member for the public. You can find out more about your rights under applicable data protection legislation from the Information Commissioner's Office website available at www.ico.org.uk.

This Policy

The School will update this policy from time to time. Any substantial changes that affect your rights will be provided to you directly as far as is reasonably practicable.

Contact and complaints

If you have any queries about this policy or how we process your personal data, or if you wish to exercise any of your rights under applicable law, you may contact your line manager or refer the matter through the staff grievance procedure.

If you are not satisfied with how we are processing your personal data, or how we deal with your complaint, you can make a complaint to the Information Commissioner: www.ico.org.uk. The ICO does recommend you seek to resolve any issues with the data controller initially prior to any referral.

Pupil and Parental Privacy Policy

This document is applicable to past and present Pupils and Parents of St Edward's School Trust Cheltenham.

This policy is intended to provide information about how the School will use (or "process") personal data about individuals including: its current, past and prospective pupils; and their parents, carers or guardians (referred to in this policy as "parents").

This information is provided because Data Protection Law gives individuals rights to understand how their data is used. Staff, parents and pupils are all encouraged to read this policy and understand the School's obligations to its entire community.

This policy applies alongside any other information the School may provide about a particular use of personal data, for example when collecting data via an online or paper form.

This policy also applies in addition to the School's other relevant terms and conditions and policies, including:

- any contract between the School and the parents of pupils;
- the School's policy on taking, storing and using images of children;
- the School's CCTV and/or biometrics policy;
- the School's retention of records policy;
- the School's safeguarding, pastoral, or health and safety policies, including as to how concerns or incidents are recorded; and
- the School's IT policies, including its Acceptable Use policy, e-Safety policy.

Anyone who works for, or acts on behalf of, the School (including staff, volunteers, Trustees and service providers) should also be aware of and comply with this policy.

Responsibility for data protection

The Bursar as Compliance Officer will deal with all your requests and enquiries concerning the School's uses of your personal data (see section on Your Rights below) and endeavour to ensure that all personal data is processed in compliance with this policy and Data Protection Law.

The School has appointed Romero Services to undertake Data Protection Officer (DPO) duties. Romero Services can be contacted by emailing dataprotection@stedwards.co.uk.

Why the School needs to process personal data

In order to carry out its ordinary duties to staff, pupils and parents, the School needs to process a wide range of personal data about individuals (including current, past and prospective staff, pupils or parents) as part of its daily operation.

Some of this activity the School will need to carry out in order to fulfil its legal rights, duties or obligations – including those under a contract with its staff, or parents of its pupils.

Other uses of personal data will be made in accordance with the School's legitimate interests, or the legitimate interests of another, provided that these are not outweighed by the impact on individuals and provided it does not involve special or sensitive types of data.

The School expects that the following uses will fall within that category of its (or its community's) "legitimate interests":

- For the purposes of pupil selection (and to confirm the identity of prospective pupils and their parents);
- To provide education services, including musical education, physical training or spiritual development, career services, and extra-curricular activities to pupils, and monitoring pupils' progress and educational needs;
- Maintaining relationships with alumni and the School community, including direct marketing or fundraising activity;
- For the purposes of donor due diligence, and to confirm the identity of prospective donors and their background;
- For the purposes of management planning and forecasting, research and statistical analysis, including that imposed or provided for by law (such as diversity analysis);
- To enable relevant authorities to monitor the School's performance and to intervene or assist with incidents as appropriate;
- To give and receive information and references about past, current and prospective pupils, including relating to outstanding fees or payment history, to/from any educational institution that the pupil attended or where it is proposed they attend; and to provide references to potential employers of past pupils;
- To enable pupils to take part in national or other assessments, and to publish the results of public examinations or other achievements of pupils of the School;
- To safeguard pupils' welfare and provide appropriate pastoral care;
- To monitor (as appropriate) use of the School's IT and communications systems in accordance with the School's Acceptable Use Policy;
- To make use of photographic images of pupils in School publications, on the School website and (where appropriate) on the School's social media channels in accordance with the School's policy on taking, storing and using images of children;
- For security purposes, including biometrics and CCTV in accordance with the School's CCTV policy;
- To carry out or cooperate with any School or external complaints, disciplinary or investigation process; and
- Where otherwise reasonably necessary for the School's purposes, including to obtain appropriate professional advice and insurance for the School.

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. These reasons will include:

- To safeguard pupils' welfare and provide appropriate pastoral (and where necessary, medical) care, and to take appropriate action in the event of an emergency, incident or accident, including by disclosing details of an individual's medical condition or other relevant information where it is in the individual's interests to do so: for example for medical advice, for social protection, safeguarding, and cooperation with police or social services, for insurance purposes or to caterers or organisers of School trips who need to be made aware of dietary or medical needs;
- To provide educational services in the context of any special educational needs of a pupil;
- To provide spiritual education in the context of any religious beliefs;
- To run any of its systems that operate on biometric data, such as for catering, printing and security
- As part of any School or external complaints, disciplinary or investigation process that involves such data, for example if there are SEN, health or safeguarding elements; or
- For legal and regulatory purposes (for example child protection, diversity monitoring and health and safety) and to comply with its legal obligations and duties of care.

Types of personal data processed by the School

This will include 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);
- biometric information, which will be collected and used by the School in accordance with the School's biometrics policy.
- 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;
- 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 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);

How the School collects data

Generally, the School receives personal data from the individual directly (including, in the case of pupils, from their parents). This may be via a form, or simply in the ordinary course of interaction or communication (such as email or written assessments).

However, in some cases personal data will be supplied by third parties (for example another School, or other professionals or authorities working with that individual); or collected from publicly available resources.

Who has access to personal data and who the School shares it with

Occasionally, the School will need to share personal information relating to its community with third parties, such as:

- professional advisers (e.g. lawyers, insurers, PR advisers and accountants);
- government authorities (e.g. HMRC, DfE, police or the local authority); and
- appropriate regulatory bodies (e.g. NCTL, the Independent Schools Inspectorate, the Charity Commission or the Information Commissioner).
- Catering providers
- Photographers
- Health care service providers
- IT Contractors
- IT software providers
- Visiting Teachers

For the most part, personal data collected by the School will remain within the School, and will be processed by appropriate individuals only in accordance with access protocols (i.e. on a 'need to know' basis). Particularly strict rules of access apply in the context of:

- medical records held and accessed only by the School nurse and appropriate staff under his/her supervision, or otherwise in accordance with express consent; and
- pastoral or safeguarding files.

However, a certain amount of any SEN pupil's relevant information will need to be provided to staff more widely in the context of providing the necessary care and education that the pupil requires.

Staff, pupils and parents are reminded that the School is under duties imposed by law and statutory guidance (including Keeping Children Safe in Education) to record or report incidents and concerns that arise or are reported to it, in some cases regardless of whether they are proven, if they meet a certain threshold of seriousness in their nature or regularity. This is likely to include file notes on personnel or safeguarding files, and in some cases referrals to relevant authorities such as the LADO or police. For further information about this, please view the School's Safeguarding Policy.

Finally, in accordance with Data Protection Law, some of the School's processing activity is carried out on its behalf by third parties, such as IT systems, web developers or cloud storage providers. This is always subject to contractual assurances that personal data will be kept securely and only in accordance with the School's specific directions.

How long we keep personal data

The School will retain personal data securely and only in line with how long it is necessary to keep for a legitimate and lawful reason. Typically, the legal recommendation for how long to keep ordinary staff and pupil personnel files is up to 7 years following departure from the School. However, incident reports and safeguarding files will need to be kept much longer, in accordance with specific legal requirements.

If you have any specific queries about how our retention policy is applied or wish to request that personal data that you no longer believe to be relevant is considered for erasure, please contact the Bursar. However, please bear in mind that the School will often have lawful and necessary reasons to hold on to some personal data even following such request.

A limited and reasonable amount of information will be kept for archiving purposes, for example; and even where you have requested we no longer keep in touch with you, we will need to keep a record of the fact in order to fulfil your wishes (called a "suppression record").

For further information, please refer to the School's Storage and Retention of Records and Documents Policy.

Keeping in touch and supporting the School

The School and/or any relevant other organisation will use the contact details of parents, alumni and other members of the School community to keep them updated about the activities of the School, or alumni and parent events of interest, including by sending updates and newsletters, by email and by post. Unless the relevant individual objects, the School will also:

- Share personal data about parents and/or alumni, as appropriate, with organisations set up to help establish and maintain relationships with the School community, such as the parents' association
- Contact parents and/or alumni by post and email in order to promote and raise funds for the School and, where appropriate, other worthy causes;
- Should you wish to limit or object to any such use, or would like further information about them, please contact the Bursar in writing. You always have the right to withdraw consent, where given, or otherwise object to direct marketing or fundraising. However, the School is nonetheless likely to retain some of your details (not least to ensure that no more communications are sent to that particular address, email or telephone number).

Your rights

Rights of access, etc.

Individuals have various rights under Data Protection Law to access and understand personal data about them held by the School, and in some cases ask for it to be erased or amended or have it transferred to others, or for the School to stop processing it – but subject to certain exemptions and limitations.

Any individual wishing to access or amend their personal data or wishing it to be transferred to another person or organisation, or who has some other objection to how their personal data is used, should put their request in writing to the Bursar.

The School will endeavour to respond to any such written requests as soon as is reasonably practicable and in any event within statutory time-limits (which is one month in the case of requests for access to information).

The School will be better able to respond quickly to smaller, targeted requests for information. If the request for information is manifestly excessive or similar to previous requests, the School may ask you to reconsider, or require a proportionate fee (but only where Data Protection Law allows it).

Requests that cannot be fulfilled

You should be aware that the right of access is limited to your own personal data, and certain data is exempt from the right of access. This will include information which identifies other individuals (and parents need to be aware this may include their own children, in certain limited situations – please see further below), or information which is subject to legal privilege (for example legal advice given to or sought by the School, or documents prepared in connection with a legal action).

The School is also not required to disclose any pupil examination scripts (or other information consisting solely of pupil test answers), provide examination or other test marks ahead of any ordinary publication, nor share any confidential reference given by the School itself for the purposes of the education, training or employment of any individual.

You may have heard of the "right to be forgotten". However, we will sometimes have compelling reasons to refuse specific requests to amend, delete or stop processing your (or your child's) personal data: for example, a legal requirement, or where it falls within a legitimate interest identified in this policy. All such requests will be considered on their own merits.

Pupil requests

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 (see section Whose Rights? below). A pupil of any age may ask a parent or other representative to make a subject access request on his/her behalf.

Indeed, while a person with parental responsibility will generally be entitled to make a subject access request on behalf of younger pupils, the law still considers the information in question to be the child's: for older pupils, the parent making the request may need to evidence their child's authority for the specific request.

Pupils aged 13 and above are generally assumed to have this level of maturity, although this will depend on both the child and the personal data requested, including any relevant circumstances at home. Slightly younger children may however be sufficiently mature to have a say in this decision, depending on the child and the circumstances.

Parental requests, etc.

It should be clearly understood that the rules on subject access are not the sole basis on which information requests are handled. Parents may not have a statutory right to information, but they and others will often have a legitimate interest or expectation in receiving certain information about pupils without their consent. The School may consider there are lawful grounds for sharing with or without reference to that pupil.

Parents will in general receive educational and pastoral updates about their children, in accordance with the Parent Contract. Where parents are separated, the School will in most cases aim to provide

the same information to each person with parental responsibility but may need to factor in all the circumstances including the express wishes of the child.

All information requests from, on behalf of, or concerning pupils – whether made under subject access or simply as an incidental request – will therefore be considered on a case by case basis.

Consent

Where the School is relying on consent as a means to process personal data, any person may withdraw this consent at any time (subject to similar age considerations as above). Examples where we do rely on consent are: biometrics, certain types of uses of images, certain types of fundraising activities. Please be aware however that the School may not be relying on consent but have another lawful reason to process the personal data in question even without your consent.

That reason will usually have been asserted under this policy or may otherwise exist under some form of contract or agreement with the individual (e.g. an employment or parent contract, or because a purchase of goods, services or membership of an organisation such as an alumni or parents' association has been requested).

Whose rights?

The rights under Data Protection Law belong to the individual to whom the data relates. However, the School will often rely on parental authority or notice for the necessary ways it processes personal data relating to pupils – for example, under the parent contract, or via a form. Parents and pupils should be aware that this is not necessarily the same as the School relying on strict consent (see section on Consent above).

Where consent is required, it may in some cases be necessary or appropriate – given the nature of the processing in question, and the pupil's age and understanding – to seek the pupil's consent. Parents should be aware that in such situations they may not be consulted, depending on the interests of the child, the parents' rights at law or under their contract, and all the circumstances.

In general, the School will assume that pupils' consent is not required for ordinary disclosure of their personal data to their parents, e.g. for the purposes of keeping parents informed about the pupil's activities, progress and behaviour, and in the interests of the pupil's welfare. That is unless, in the School's opinion, there is a good reason to do otherwise.

However, 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, the School may be under an obligation to maintain confidentiality unless, in the School's opinion, there is a good reason to do otherwise; for example where the School believes disclosure will be in the best interests of the pupil or other pupils, or if required by law.

Pupils are required to respect the personal data and privacy of others, and to comply with the School's Acceptable Use Policy, Information Security Policy and the School rules.

Data accuracy and security

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 please notify the Bursar of any significant changes to important information, such as contact details, held about them.

An individual has the right to request that any out-of-date, irrelevant or inaccurate or information about them is erased or corrected (subject to certain exemptions and limitations under Data Protection Law): please see above for details of why the School may need to process your data, of who you may contact if you disagree.

The School will take appropriate technical and organisational steps to ensure the security of personal data about individuals, including policies around use of technology and devices, and access to School systems.

All staff and Trustees will be made aware of this policy and their duties under Data Protection Law and receive relevant training as necessary.

This policy

The School will update this policy from time to time. Any substantial changes that affect your rights will be provided to you directly as far as is reasonably practicable.

Queries and complaints

Any comments or queries on this policy should be directed to the Bursar via the School Bursary.

If an individual believes that the School has not complied with this policy or acted otherwise than in accordance with Data Protection Law, they should utilise the School complaints/grievance procedure and should also notify the Bursar. You can also make a referral to or lodge a complaint with the Information Commissioner's Office (ICO), although the ICO recommends that steps are taken to resolve the matter with the School before involving the regulator.

Storage and Retention of Records and Documents Policy

The following retention table sets out the School's policy on retention periods. The retention periods will be reviewed annually to ensure compliance with the law in force at that time.

Type of Record/Document	Retention Period
EMAILS ON SERVER	*NB – this will generally include personal data*
1. Pupil email account	1. Delete upon leaving school, or within one year.
2. Staff emails	2. Routine deletion of historic emails after 3 years and delete account within 1 year of leaving school.
SCHOOL-SPECIFIC RECORDS	
1. Registration documents of School 2. Attendance Register 3. Minutes of Trustees' meetings 4. Annual curriculum	1. Permanent (or until closure of the School) 2. 6 years from last date of entry, then archive. 3. 6 years from date of meeting 4. From end of year: 3 years (or 1 year for other class records: eg marks / timetables / assignments)
INDIVIDUAL PUPIL RECORDS	*NB – this will generally be personal data*
1. Admissions: application forms, assessments, records of decisions	1. 25 years from date of birth (or, if pupil not admitted, up to 7 years from that decision).
2. Examination results (external or internal)	2. 7 years from pupil leaving School
3. Pupil file including: 3.1 Pupil reports 3.2 Pupil performance records 3.3 Pupil medical records	3. 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).
4. Special educational needs records (to be risk assessed individually)	4. Date of birth plus up to 35 years (allowing for special extensions to statutory limitation period)
SAFEGUARDING	*NB this will contain personal data*
1. Policies and procedures	1. Keep a permanent record of historic policies
2. DBS disclosure certificates (if held)	2. No longer than 6 months from decision on recruitment, unless DBS specifically consulted – but a record

3. Accident / Incident reporting	of the checks being made must be kept, if not the certificate itself. 3. Keep on record for as long as any living victim may bring a claim (NB civil claim limitation periods can 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.
4. Child Protection files	4. 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).
5. Video recordings of meetings	5. Where e.g. one-on-one meetings of classes, counselling, or application interviews are recorded for safeguarding purposes, a shorter-term retention policy is acceptable based on the DSL's view of how quickly a concern will likely be raised: e.g. 3-6 months or immediately upon DSL review.

CORPORATE RECORDS

1. Certificates of Incorporation	1. Permanent (or until dissolution of the company)
2. Minutes, Notes and Resolutions of Boards or Management Meetings	2. Minimum – 10 years
3. Shareholder resolutions	3. Minimum – 10 years
4. Register of Members/Shareholders	4. Permanent (minimum 10 years for ex- members/shareholders)
5. Annual reports	5. Minimum 6 years

ACCOUNTING RECORDS

1. 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)	1. Minimum – 3 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
2. Tax returns	2. Minimum 6 years
3. VAT returns	3. Minimum 6 years
4. Budget and internal financial reports	4. Minimum 3 years

CONTRACTS AND AGREEMENTS

1. Signed or final/concluded agreements (plus any signed or final/concluded variations or amendments)	1. Minimum – 7 years from completion of contractual obligations or term of agreement, whichever is the later
2. Deeds (or contracts under seal)	2. Minimum – 13 years from completion of contractual obligation or term of agreement

INTELLECTUAL PROPERTY RECORDS

1. Formal documents of title (trade mark or registered design certificates; patent or utility model certificates)	1. Permanent (in the case of any right which can be permanently extended, eg trade marks); otherwise expiry of right plus minimum of 7 years.
2. Assignments of intellectual property to or from the School	2. As above in relation to contracts (7 years) or, where applicable, deeds (13 years).
3. IP / IT agreements (including software licences and ancillary agreements eg maintenance; storage; development; coexistence agreements; consents)	3. Minimum – 7 years from completion of contractual obligation concerned or term of agreement

EMPLOYEE/PERSONNEL RECORDS *NB this will contain personal data*

1. Single Central Record of employees	1. Keep a permanent record of all mandatory checks that have been undertaken (but <u>not</u> DBS certificate itself: 6 months as above)
2. Contracts of employment	2. 7 years from effective date of end of contract
3. Employee appraisals or reviews	3. Duration of employment plus minimum of 7 years
4. Staff personnel file	4. As above, but <u>do not delete any information which</u> <u>may be relevant to historic safeguarding claims</u>.
5. Payroll, salary, maternity pay records	5. Minimum – 6 years

6. Pension or other benefit schedule records	6. Possibly permanent, depending on nature of scheme
7. Job application and interview/rejection records (unsuccessful applicants)	7. Minimum 3 months but no more than 1 year
8. Staff immigration records (Right to work, etc.)	8. Minimum – 2 years from end of employment
9. Tier 2 migrant worker sponsor records	9. Minimum – 4 years
10. Health records relating to employees	10. 7 years from end of contract of employment
11. Low-level concerns records about adults	11. Regular review recommended in order to justify longer-term retention as part of safeguarding files.
INSURANCE RECORDS	
1. Insurance policies (will vary – private, public, professional indemnity)	1. 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.
2. Correspondence related to claims/ renewals/ notification re: insurance	2. Minimum – 7 years (*but this will depend on what the policy covers and whether e.g. historic claims may still be made*)
ENVIRONMENTAL, HEALTH & DATA	
1. Maintenance logs	1. 10 years from date of last entry
2. Accidents to children	2. 25 years from birth (longer for safeguarding)
3. Accident at work records (staff)	3. Minimum – 4 years from date of accident, but review case-by-case where possible
4. Staff use of hazardous substances	4. Minimum – 7 years from end of date of use
5. Covid-19 risk assessments, consents etc. (*for now: this to be subject to further review*)	5. Retain for now legal paperwork (consents, notices, risk assessments) but not individual test results
6. Risk assessments (carried out in respect of above)	6. 7 years from completion of relevant project, incident, event or activity.
7. Art.30 GDPR records of processing activity, data breach records, impact assessments	7. No limit: as long as up-to-date and relevant (as long as no personal data held)

Taking, Storing and Using Images of Children Policy

1. This Policy

- This Policy 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 Edward'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 terms and conditions, 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. Images of pupils in a safeguarding context are dealt with under the School's relevant safeguarding policies.

2. General points to be aware of

- 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.

- Parents who accept a place for their child at the School are invited to indicate agreement to the School using images of him/her as set out in this policy via the School's terms and conditions and/or from time to time if a particular use of the pupil's image is requested. 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).

- 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.

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

- 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.

3. Use of Pupil Images in School Publications

- 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:

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

- in communications with the School community (parents, pupils, staff, Trustees and alumni) including by email, on the School intranet and by post;

- 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

- 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.

- 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. Use of Pupil Images for Identification and Security

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

- 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 CCTV Policy and any other information or policies concerning CCTV which may be published by the School from time to time.

5. Use of Pupil Images in the Media

- 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.

- 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.

6. Security of Pupil Images

- 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.

- 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.

- 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.

7. Use of Cameras and Filming Equipment (including mobile phones) by Parents

- 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:

    - 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.

    - 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.

    - 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.

    - 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.

    - 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.

- 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.

- 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.

8. Use of Cameras and Filming Equipment by Pupils

- 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.

- 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.

- 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, e-Safety Policy, IT Acceptable Use Policy, 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.

CCTV Policy

The purpose of this policy is to regulate the management and operation of the Closed Circuit Television (CCTV) System at St Edward's School Trust Cheltenham (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).

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. For further guidance, please review the Information Commissioner's CCTV Code of Practice (accessible here [link]).

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.

1. Objectives of the System

- 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 in line with the School's code of conduct.
- To monitor and uphold discipline among pupils in line with the School Rules, which are available to parents and pupils on request.

2. Positioning

- 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.
- 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.

3. Maintenance

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

4. Supervision of the System

- Staff authorised by the School to conduct routine supervision of the System may include Porters, day or night security, supervisors at the sports centre and relevant staff on duty.
- 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.

5. Storage of Data

- The day-to-day management of images will be the responsibility of the IT Infrastructure Manager who will act as the System Manager, or such suitable person as the System Manager shall appoint in his or her absence.
- Images will be stored for 2-4 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.
- 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 logged.

6. Access to Images

- 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).
- Individuals also have the right to access personal data the School holds on them (please see the Data Protection Policy), 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.
- 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 Head/Bursar, 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 6.2 above;
- To the School's insurance company where required in order to pursue a claim for damage done to insured property; or
- In any other circumstances required under law or regulation.

- Where images are disclosed under 6 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).

7. Other CCTV systems

- The School does not own or manage third party CCTV systems but may be provided by third parties (such as other Schools) with images of incidents where this in line with the objectives of the School's own CCTV policy and/or its School Rules.
- Many pupils travel to School on coaches provided by third party contractors and a number of these coaches may be 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. Complaints and queries

- 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 Bursar.

CCTV Footage Access Request

The following information is required before the School can provide copies of or access to CCTV footage from which a person believes they may be identified.

Please note that CCTV footage may contain the information of others that needs to be protected, and that the School typically deletes CCTV recordings after 2 - 4 weeks.

Name and address: (proof of ID may be required)	
Description of footage (including a description of yourself, clothing, activity etc.)	
Location of camera	
Date of footage sought	
Approximate time (give a range if necessary)	

Signature*……

Print Name…… Date ……..

* NB if requesting CCTV footage of a child under 13, a person with parental responsibility should sign this form. For children 13 or over, the child's authority or consent must be obtained except in circumstances where that would clearly be inappropriate and the lawful reasons to provide to the parent(s) outweigh the privacy considerations of the child.

Biometric Data Policy

Background

Biometric data is personal information about an individual's physical or behavioural characteristics that can be used to identify that person; this can include their fingerprints, facial shape, retina and iris patterns, and hand measurements. This does not include photographs, other than where a child's photograph is automatically scanned by an automated biometric recognition system to provide him or her with a service in the School.

St Edward's Senior School uses Biometric data for its cashless catering service as well as its print management system. Biometric data is not used in the Preparatory School.

Consent

Written consent is required from at least one parent for all pupils under the age of 18 where biometric information is used.

The School will respect pupils' wishes if they refuse to participate in the biometric system. A pupil's objection will always override parental consent in this regard, and indeed the objection of one parent can override the consent of another. Consent may also be withdrawn at any stage.

Consent may be withdrawn at any time by contacting the Headteacher's PA in writing.

Reasonable alternatives

The Protection of Freedoms Act 2012 dictates that "reasonable alternative arrangements" must be provided for pupils who do not use automated biometric recognition systems either because their parents have refused consent (or a parent has objected in writing) or due to the pupil's own refusal to participate.

The alternative arrangements will ensure that pupils do not suffer any disadvantage or difficulty in accessing services/school premises etc. as a result of their not participating. Likewise, such arrangements should not place any additional burden on parents whose children are not participating in such a system.

If parents or pupils do not provide consent for their biometric data to be used, a keypad will be provided which pupils can use their own unique pin code.

Use of Pupils' Biometric Data by the School

In accordance with the Protection of Freedoms Act 2012, the School requires your consent to take and use information from your child's fingerprint as part of an automated biometric recognition system. This biometric information will be used by the School for the following purposes:

- To enable pupils to buy food & drink if they wish
- To enable pupils to use print services

The data that is held will not be used by any other organisation for any other purpose, except solely as necessary for the purposes stated above (for example, if the School's IT or security providers need to process the information) and the School will not use the biometric information for any reason other than those stated above.

Please see the School's Privacy Policy for further information about how the School uses your child's personal data generally.

If you object to the use of your child's biometric data in this way, the School will provide a workaround to the system without using biometrics. Once your child stops using the biometric recognition system, his/her biometric information will be securely deleted by the School in accordance with the Information Commissioner's guidance.

Parental consent to use of biometric data

Please indicate below if you understand the above and are happy to consent for the time being to your child's biometric data being used in the above ways. You may withdraw consent at any time in the future by contacting the Headteacher’s PA in writing.

Your consent will continue until the child either leaves the S chool or stops using the system.

Yes, I understand and consent to the above

Signed: _____

Name of parent/guardian: _____

If you object to such uses until further notice, please indicate below. In ensuring we can give effect to your wishes, it will also assist us if you are able to give reasons.

Reasons:

Data Breach Procedure

This policy assumes that the criteria for reporting breaches to the ICO are understood -in short, this means that Recital 87 of the GDPR makes clear that when a security incident takes place, you should quickly establish whether a personal data breach has occurred and, if so, promptly take steps to address it, including telling the ICO if required.

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.

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 if the breach will result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage. Such matters may separately require a report to the Charity Commission but caution will be taken with which organisation the data protection duty lies as Serious Incident reports are subject to Freedom of Information requests which may, if answered, create a further data or privacy breach if the lines of responsibility are not clear.

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.

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.

Or, use the security breach notification form, which should be sent to the email address: casework@ico.org.uk
or by post to the ICO office address: Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF.

Data Protection Guidance

The following does not constitute part of this Policy and is intended for guidance purposes only.

Storage and Retention of Records and Documents Guidance

Legal note 1: The legal framework around document retention in the UK

The UK Data Protection Act 2018 (**DPA**) and General Data Protection Regulation (**GDPR**), which will remain part of UK law following Brexit, did not fundamentally change the principles for the length or lawfulness of document retention. The rule is still a question of necessity for a particular purpose, although it draws in further questions around data security, erasure or access requests, and cost. The new legislation did, however, introduce more exacting standards about use and storage of personal data generally, more rights for individuals, and greater penalties for contraventions or data breaches – with the practical effect of requiring more dynamic, efficient and secure storage systems, and greater accountability for what is collected and kept. The key considerations are as follows:

- All information held by schools needs to be justifiable, by reference to a lawful purpose;
- Schools must be transparent and accountable to individuals as to what they hold;
- Schools must understand and be able to explain to regulators the reasons why they hold data – which also means keeping records of how decisions around personal data are made;
- Schools must be prepared to respond more readily to data subject requests. As well as the right of subject access, schools must be able to amend, delete or transfer data promptly upon any justified request, or otherwise prepared to explain why they will not do so;
- It should be possible to audit how the personal data you hold was collected, and when; and
- Sensitive data (notably special category data, including around health and pastoral matters, or criminal allegations) must be held securely and accessed only by those with reason to view it. In many cases schools will need an "appropriate policy document"[1] explaining why it is kept.

***Please note** that different rules and considerations will apply to genuine archiving (where a record has been designated for retention in a formal archive due to its enduring value, as explained here). Schools should consider one of two actions at the end of a document's "life": either secure deletion, or archiving.*

A school's purposes for retaining data must be explained to those affected – parents, pupils, staff, past and present – although that is not to say a school's specific data retention schedule needs to be public. However, under GDPR the basic principles and rationale applied in terms of retention do need to be communicated as part of its Privacy Notice. The ISBA's template notice can be found here.

The GDPR requirement on organisations to document their processing activities (i.e. under Article 30 GDPR, to keep a record of what they do with what data, and why) is separate from the considerations of this note, which deals with questions of how long to retain the data itself, and why. The Information Commissioner's Office (**ICO**) has produced guidance around the documentation process here and here, and has provided templates here. We provide these for completeness but they do not form part of this guidance note or policy: and because such Art.30 "Records of Processing Activities" do not contain personal data of any identifiable individuals, they should be kept indefinitely as legal records, but updated as required from time to time.

[1] Where required by Sch.1 the Data Protection Act 2018 (and as defined therein): the ICO has a template here.

Legal note 2: IICSA, child protection and document retention

When the Independent Inquiry into Child Sexual Abuse (IICSA) was launched, its then-chair made some forceful statements about document retention. Alongside various high-profile safeguarding cases, all independent schools will be aware of the emphasis that was placed on long-term, lifetime or even indefinite keeping of full records related to incident reporting. Whilst we still await the final conclusions of IICSA, many schools will be extending this rule on a 'safety first' basis to all personnel and pupil files.

This note has been drafted in full awareness of these considerations. Whether or not a core participant in the inquiry, it is strongly to be recommended in the current climate that schools do not embark on a policy of deleting historic staff and pupil files, or any material potentially relevant for future cases, even if that data has been held for long periods already. Data protection issues should never put child safety at risk, nor take precedence over the general prevention and processing of safeguarding claims.

What should also be emphasised, however, is that the present focus on safeguarding does not mean that existing laws in respect of data protection or confidentiality are now in suspension, nor that schools may not still be liable for breaches of data protection legislation (such as retaining personal data longer or in greater volume than *is necessary for its purpose*, or a failure to keep the data accurately or safely). Schools will already find support in data protection law for lifetime retention of adequate and accurate records where they are of potential relevance to historic cases, for which legal limitation periods may be set aside, or of potential future value to victims. However, schools should be aware that the longer they hold large amounts of personal data, the more onerous their exposure to subject access rights (individual requests for data) and data breach. Sensitive personal data of employees or pupils, including allegations of a sexual or criminal nature (whether proven or not) – or details as to physical or mental health – should be kept securely, shared with or accessible to proper persons on a need-to-know basis.

Historic insurance documents, which are not likely to contain personal data, should be retained indefinitely. Regarding pupil and personnel files, each school may wish to take a different view; but where the school is on notice of possible concerns or incidents involving the pupil or staff member in question, longer retention periods than set out in the below schedule may be recommended. See also specific provision in the below table concerning low-level concerns recording and video records. In due course we expect more settled guidance from the relevant authorities, and IICSA once concluded, on best practice for longer-term retention. If practical resources mean that it is not feasible to conduct a thorough and regular review, then schools should in the current climate err on the side of retention, rather than disposal, of staff and pupil files. In the meantime, the threat of historic abuse claims and the safeguarding value of child protection records will generally outweigh the costs and risks of retaining such records in line with data protection obligations.

Legal note 3: child protection files and KCSIE

When schools pass on a **child protection file** to a new school, as Keeping Children Safe In Education (KCSIE) requires when a pupil under 18 is transferred, some DSLs and local authorities advise that schools should delete their own copy. That is not the view of ISBA's legal advisers. Whilst this may be appropriate for maintained schools (where a single copy will be kept within the local authority system), for independent schools in the current environment – in light of IICSA's statement and possible future claims against the school – it is a clear risk to delete any records of incidents that occurred while the pupil was at the school, or any information that was relevant to what action

the school took. That applies just as it would for a pupil leaving the school at the normal academic age. Schools must balance that risk against any risk of seeming to demur from local authority advice or guidance, and also consider in the relevant circumstances exactly what needs to be shared and/or retained from the file.

The purpose of this note

Schools will generally seek to balance the benefits of keeping detailed and complete records – for the purposes of good practice, archives or general reference – with practical considerations of storage, space and accessibility. The following legal considerations apply to independent schools in respect of retention of records and documents which must be borne in mind. These include:

- statutory duties and government guidance relating to schools, including e.g. KCSIE;
- disclosure and evidence requirements for potential future litigation;
- contractual and insurance obligations;
- the laws of confidentiality and privacy; and (last but by no means least relevant)
- GDPR and the DPA, which enshrines it in UK law.

These will inform not only minimum and maximum retention periods (the rationale for which should be notified to data subjects via privacy notices and, for more sensitive personal data, recorded in appropriate policy documents), but also what to keep and who should be able to access it.

Striking a balance

Even justifiable reasons to keep certain records, such as child protection records, for many years after pupils or staff leave the school will need to be weighed against personal rights. The longer potentially relevant personal data is retained, and the more sensitive material is kept on file, the greater the administrative burden on schools, in terms of both secure storage and individual subject access rights.

Steps a school can take to support its retention policies are (a) communicating the reasons for the policy in privacy notices and staff or parent contracts; and (b) ensuring any records necessary to keep long-term are kept very secure, accessible only by trained staff on a need-to-know basis.

1. Meaning of "Record"

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 GDPR.

An obvious example of a record containing personal data would be a database (such as a mailing list or the staff Single Central Record), or a pupil or personnel file specific to an individual. However, a "record" of personal data could arise simply by holding an email on the school's systems: your policies should ensure staff do not use email accounts or inboxes as proxy filing systems for key documents.

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 for retention purposes than its contents, and the reason for keeping it (although format is of course an important consideration in terms of how best to preserve documents securely).

Digital records

Many schools who have historically relied on paper records will have been going through a process of digitisation of existing records, perhaps over a number of years. This is generally to be encouraged.

However, digital records can be lost or misappropriated in huge quantities very quickly. Access to sensitive data – or any large quantity of data – should as a minimum be password-protected (ideally with two-factor authentication), with internal access on a need-to-know basis. Where 'cloud storage' or intranet access is used, consider what data needs to be made available to which users.

If personal information of any volume or sensitivity is permitted to be kept on personal devices, **digital encryption** is essential. That will usually be the difference between a lost laptop being a simple matter of the cost of the device, or a serous reportable data breach.

Email accounts and internal messaging systems

Emails – whether they are retained electronically or printed out as part of a paper file – are also "records" likely to contain personal data (of the sender, recipient, or a third party) in their body, footer, in the sent/received fields, or in attachments.

They may also contain particularly important information: whether as disclosable documents in any litigation, or as representing personal data of the sender (or subject) in a subject access request. Again, however, school policy and training should mitigate against using email accounts as proxy filing systems. It is our view that short term email retention policies of no more than 2 or 3 years – whether imposed on staff centrally, or as a requirement for each staff member to follow – will encourage the correct habits in terms of not relying on email accounts to retain important information, resources, contracts, legal advice, attendance notes or incident reports that ought to be properly held elsewhere (i.e. in the appropriate file, by the appropriate person).

Such policy and training must also stress to staff the great importance of care and professionalism in how such records are created by casual email (or other forms of instant messaging such as Team or Slack, which are also records for these purposes). This will become particularly apparent when a subject access request is made by a colleague, pupil or parent.

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 – or its deletion. Metadata may be necessary to examine under a legal claim or a data audit.

Records on personal devices including SMS / WhatsApp

Whether text / WhatsApp messages, and any other files or notes held by a staff member or governor on their personal device (including tablet or smartphone) counts as a school “record” will depend on the circumstances. As a general rule, an employee has an expectation of privacy in their own messaging for personal use, and is not subject to GDPR for solely domestic or ‘household’ uses of data.

However, where personal devices are used by employees or governors / trustees / board members for official school use – for example to discuss a pupil issue, parental complaint or disciplinary matter – it may be deemed an official record of the school. This means it may be disclosable in litigation or under a subject access request, if the school has reasonable grounds to believe relevant evidence or personal data might be found on the device, including by SMS, WhatsApp or personal email. In that sense, any staff or governor WhatsApp group must be used with the same professional formality as email.

What the school policy says about use of personal devices or messaging for official schools purposes will be a factor in assessing whether they are to be deemed searchable records. If staff members or governors are using their devices contrary to official policy, there are grounds to argue these should not be deemed school records under school control. Where schools seek to impose common-sense rules around how to use personal devices, what is acceptable “personal” use of school systems, and how to manage data on them, this has clear benefits but risks accepting formal responsibility for their use.

Video / audio recordings

Particularly given the recent rise of remote provision of lessons, meetings, assessments and interviews, schools are increasingly capturing many gigabytes of personal data (some of it impactful and personal).

The reasons for recording such virtual sessions my vary: from seeking to keep a record as a resource for those unable to attend at the time (notably for group or assembly sessions), via classes where a child was absent (e.g. owing to having to self-isolate), down to safeguarding reasons (e.g. for one on lessons, VMT or counselling sessions, or application interviews). This throws up many issues, some of which are dealt with in this (Covid-specific) ISBA/Farrer & Co note, but one of them is retention.

Such recordings are also digital records and – depending to a degree on both their contents and how they are stored / tagged – may be deemed the personal data of anyone identifiable from the recording. How long they may be kept, therefore, should be judged in the same way any other type of record is: for what purpose is it kept, and how long is it necessary to keep it?

Some confusion has been caused by schools having notified users or parents that recordings are being kept for safeguarding purposes, and (as stated in some cases) for those purposes only. This can create issues if the recording is then needed for some other disciplinary, complaint or training purpose; it can also cause confusion as to how long a recording needs to be kept, with many schools operating a blanket policy of preserving all safeguarding-related records indefinitely.

However, common sense dictates that not all such recordings will be necessary for long-term legal or safeguarding purposes. In practice, this would be expensive and unmanageable in storage terms, and could create unnecessary burdens (subject access rights, for example) and data security risks. Your school senior leadership team, DSL and IT teams should collectively agree what a feasible storage period is *based on what is a likely period in which a complaint or concern will generally be raised* following a virtual lesson or meeting (or when reviews or spot checks will be carried out, if sooner). This should be led by the safeguarding advice but – unless something arises that means it should be treated as a record of an incident – is unlikely to be more than 3 months. A similar approach may already be in place for short-term CCTV recording storage and review: see the ISBA CCTV policy and guidance note.

Paper records

Paper records are most often damaged by damp or poor storage conditions; but as well as applying common sense (i.e. dry, cool, reasonable ventilation, no direct sunlight; avoid storing with metals, rubber or plastic which might deteriorate or damage the paper), security is also vital – especially if the materials contain legally or financially sensitive data, as well as data personal to individuals.
Under GDPR, paper records are only classed as personal data if held in a qualifying "filing system". This means organised, and/or indexed, such that specific categories of personal information relating to a certain individual are readily accessible – and so searchable much as a digital database might

be. By way of example, personnel files searchable by marked dividers will likely fall under within GDPR. A daily notebook, or diary, or chronological file of correspondence may not, unless it is readily clear to whom the file or notebook substantially relates: for example, a complaint or case file.
However, schools should not be tempted to retain or store personal data in disorganised or inaccessible hard copies, except as part of an appropriate archiving policy (which may be subject to an exemption from data protection rules around access and erasure in any event: see below). Schools are likely to remain responsible, as a principle of data security, for personal information contained on handwritten notes, print-outs taken from electronic files, or disclosures from their systems made orally. Remember: data protection law is only one consideration in retaining records, and it is far preferable for governance and legal reasons to keep paper documents ordered and accessible.

2. A note on "personal data": what it is, and when it is lawful to retain

Aside from purely charitable, corporate, estate or financial records (including asset lists, IP, accounts, contracts etc.), most records will contain information about living[2] individuals: e.g. pupils, parents, alumni, governors, staff (past, present and prospective), and consultants / contractors / VMTs. You will also likely hold professional contacts, including at other schools or local authorities, and supporter / donor lists. That type of information is likely to amount to "personal data" for these purposes, and therefore be subject to data protection laws which necessarily interact with these 'document retention' guidelines.

Generally, the sources of law that determine how long you retain personal data will not be GDPR or the DPA, but derive from elsewhere: eg statutory time limits by which legal claims must be made; the stipulations of your contracts; or the requirements of governmental organisations (e.g. the Disclosure and Barring Service, Charity Commission, IICSA etc.). As a general rule, in the event of any doubt or apparent contradiction with data protection law, statutory legal duties (including those under KCSIE / safeguarding) should be followed. However, data protection law is the overarching legal framework here and – properly understood and applied – does accommodate all these statutory duties on schools.

What data protection law requires is simply that personal data is only retained for as long as necessary – and only as much as is necessary – for the specific lawful purpose (or purposes) it was acquired, or at least for clearly compatible purposes[3]. This will of course vary and, in accordance with the policies and processes adopted by your school, may be either shorter or longer than the suggested document retention period, according to context. This enters an area of context and judgment which may therefore require tailored, specific policy-making by your school on a case-by-case basis.

3. What is a lawful purpose to hold and retain personal data?

Most “ordinary” personal data may be processed in connection with a private contractual duty (e.g. under an employment or parent contract) or where necessary for a “legitimate interest” as defined in GDPR (which ought to be set out in your school’s privacy notice). It may then be retained for a reasonable and necessary period of time afterwards, generally linked to legal claims.
However, a higher standard would apply to the processing of "*special category* [= sensitive] personal data", including notably health, trade union membership, ethnicity, religious beliefs, political views

[2] Data protection rights and obligations do not apply to deceased individuals, even though they may be identifiable. Therefore lifetime retention periods, in terms of GDPR applicable, may equate to permanent retention.
[3] This may include archiving in the public interest and statistical record-keeping, with suitable safeguards.

and sexual life. Similar rules apply to any records of criminal proceedings, offences or allegations. A mere contractual need to process, or a legitimate interest of the school or third party, would not in itself justify the retention of such personal data – but if it were necessary in connection with the defence of future legal claims, or to help prevent or detect crime or unlawful behaviour, or as part of the school's safeguarding duties, then a lawful GDPR or DPA basis to retain will arise.

4. Archiving, data management, and the destruction or erasure of records

All staff should receive basic training in data management – issues such as security, recognising and handling sensitive personal data (alongside training in safeguarding and first aid, etc.) – at least every two years, in accordance with ICO guidance. Staff given specific responsibility for the management of records must have specific training and ensure, as a minimum, 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;

- important records, and large or sensitive personal databases, are not left sitting in email accounts, 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). Where this is absolutely necessary, it should be subject to a risk assessment and in line with an up-to-date IT use policy;

- questions of back-up or migration are likewise approached in line with general school policy (such as professional storage solutions or IT systems) and not individual *ad hoc* action;

- arrangements with external storage providers – whether physical or electronic (in any form, but most particularly "cloud-based" storage), and in whatever territory – are supported by robust, GDPR-compliant contractual arrangements providing for secure control, access and retrieval;

- 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

- 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.

This is particularly important in respect of the school's specific legal obligations under GDPR. However, they amount to common sense rules even where personal data is not directly involved.
Please be aware of the difference between *archiving* and *retention for a "live" purpose*, and refer to the SARA/ISBA note here. Record keeping for potential (rather than known) legal claims is a "live" purpose.

4. A note on litigation and limitation periods for claims

One consideration in whether it is necessary (or prudent) to keep records is possible future litigation. Generally speaking, an institution will be better placed to deal with claims if it has a strong corporate memory – including adequate records to support its position, or a decision that was made. Guidance from the ICO has suggested that records relevant to duties of care (for example, allergy information) may be processed on grounds of being necessary for defence of future legal claims. This is supportive to some degree of a "just in case" policy, but reasonable judgment should be exercised

– especially where the data retained is impactful, surprising, or if an individual has reasonably objected.

Ideally, key records would not be disposed of until the limitation period for bringing a claim has passed. In respect of these periods, and how they are reflected in the template schedule, please note:

- In some cases the “clock” may begin with a specific event, or when the claimant became aware of it; or it may be the end of a calendar year; but a school’s review of any documents marked for deletion may be conducted annually at the end of a school year. Therefore, for the purpose of this guidance a contingency is generally built in: ie 7 years where the statutory limitation is 6.

- For most contracts the limitation will be 6 years from any breach (but 12 years in case of a witnessed deed), so the date to start counting from is the last day of the period under contract.

- The period of 6 years also applies to many claims outside contract (such as fraud, mistake or many common types of negligence / duty of care claim, from when the cause arose).

- In the case of personal injury, and some other types of negligence claims, it is only 3 years. However, if the harm is only discovered later – eg 'latent' damage, or some unseen injury – then the timer only starts from the point of discovery: subject, in the case of latent property damage, to a 15-year backstop. See further below regarding historic abuse claims.

- Where termination of employment of a staff member is concerned, contractual claims may be brought up to 6 years later. For discrimination cases (which can of course apply to applications, and indeed pupils) it is usually only 3 months: however, where a contractual relationship was formed, the longer contractual period for claims will provide the necessary limitation backstop.

- Where there has been early exclusion of a pupil from the school, a parent may bring a claim under the parent contract for 6yrs from the point of termination. Be aware that application processes (for pupils) have a contractual element, although it is probably excessive to keep unsuccessful applications for the full 6/7 years unless the school is aware of a likely claim.[4]

- For pupils, limitation periods will only apply from when they reach the age of 18, and they may bring a negligence claim separately to their parents (hence the rule of 25 years from birth).

Insurance documents will not be personal data and relevant historic policies need to be kept for as long as a claim might arise. Finally, limitation periods may be disapplied altogether by courts in the case of certain crimes or associated breaches of care (e.g. historic abuse), whether a charge is brought by the police or a school is sued under a private claim. It is not always possible to try a case where the evidence is inadequate, including due to a lack of corporate memory (e.g. records and witnesses). However, as recent cases and IICSA (the Independent Inquiry into Child Sexual Abuse) have shown, authorities will expect to see a full and proper record and inferences may be drawn otherwise.

[4] There may be administrative reasons for keeping records of applications beyond conclusion of the entry process: for example, if the pupil might try entry again the following cycle (i.e. within 1 year) or at a later entry stage. Such a policy should be notified at the point of application together with the chance to object.

Often these records will comprise personal or sensitive personal data (e.g. health or criminal allegations). In such instances, even justifiable reasons to keep records for many years will need to be weighed against personal rights. Recent 'historic' cases in the field of child protection make a cautious approach to record retention advisable and, from a GDPR perspective, make it easier for a school to justify retention for long periods – even the lifetime of a pupil. The most important steps a school can take to support such a policy are (a) having adequate policies explaining the approach, including notices in both staff and parent contracts; and (b) ensuring any long-term records worth keeping are kept very secure, accessible only by trained staff on a need-to-know basis.

5. The risks of longer retention

Notwithstanding the legal grounds and (in some cases) imperatives to do so, the longer potentially relevant personal data is retained, and the more sensitive material is kept on file, the greater the administrative and storage burden on schools. This also increases the amount of material in respect of which schools must be accountable to data subjects (e.g. information requests, "right to be forgotten" requests), and the consequences of data security breach become more serious.
Schools must take professional advice and decide for themselves where to draw the line in retaining data for these purposes: some may err on the side of caution and retain; others will apply a clear system for filleting pupil or personnel files, or indeed email folders, down to the information they think is likely to be relevant in the future. However, this is a decision that should always be made mindful of risk and knowledge of where historic incidents may have occurred or future complaints may arise. It is also vitally important that all records handlers bear in mind, when creating documents and records of any sort (particularly email, but also video meeting recordings and internal staff messaging systems), that at some point in the future those documents and records could be disclosed – whether as a result of litigation or investigation, or because of a subject access request under GDPR. The watchwords of record-keeping are therefore accuracy, clarity, professionalism and objectivity.

6. A note on secure disposal of documents and devices

For confidential, sensitive or personal information to be considered securely disposed of, it must be in a condition where it cannot either be read or reconstructed. For **hard copy** documents, skips and 'regular' waste disposal will not be considered secure. Paper records or images should be shredded using a cross-cutting shredder; devices for digital storage and recordings should be dismantled or broken into pieces. Where third party disposal experts are used they should ideally be supervised but, in any event, under adequate contractual obligations to the school to process and dispose of the information.

For **digital devices**, a number of individual steps are advisable prior to disposal: wiping the hard drive and/or activating drive encryption; uninstalling and/or deauthorising applications or accounts that could enable a user to access secure school systems (including wiping browsing history and cookies); and/or physically destroying the drive with a drill or hammer. Policies will be different according to whether devices are being recycled between staff or disposed of, but where schools allow a policy of using “own devices” then it must be clear that the same disposal polices apply to them, and that school IT support will be available if assistance is needed in safely destroying, wiping or readying devices for others.

Data Breach Guidance

FAQs

Do we have to report every data breach?
Not necessarily, although you are certainly expected to record them internally – and it is strongly advisable to include a record of how it was assessed, what steps were undertaken and why the decision was made not to report. This will be useful later if there are unanticipated consequences.

The ICO not want to be appraised of every “Reply All” email, temporary system outage, or every loss of an encrypted device. At the same time, the intention of the new reporting regime is not to generate more fines and enforcement notices, but (in line with wider government policy) to help the ICO gather statistical data on the patterns of UK data breaches. So not all reporting should be feared: see the ICO's blog here.

What is the threshold and timescale for notifying the ICO?
"…without undue delay and, where feasible, not later than 72 hours after having become aware of it… unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons."

As above, this is changing for GDPR. Under the previous regime it was common first to inform the individuals affected, and gauge their reaction, before deciding whether or not to involve the ICO. From 25 May this will rarely be feasible within the 72-hour timeline allowed for notification, absent a reason for delay. One such reason might previously have included consulting with those affected to assess the likely harm: but under GDPR the threshold for notifying the ICO is in fact lower than for notifying individuals, hence this may need to come sooner in the process.

Schools which are charities should keep in mind that any report made to another regulator ought routinely to be backed up with a report to the Charity Commission. This tends to result in a very soft, hands-off response for all but the most serious breaches. It may be in due course that this practice will change in respect of more minor data breach reporting: but until otherwise notified, this should continue as before under GDPR.

What is the threshold and timescale for notifying affected individuals?
"when likely to result in a high risk to the rights and freedoms of natural persons… without undue delay."
Communication of the breach to those affected is only strictly necessary if the likely harm is high risk: whether from embarrassment or loss of privacy, or exposure to fraud. There is both a reputational and a legal sensitivity to how this is handled. Individuals are likely to be increasingly aware of the right to bring group claims. Such claims may be low-value, but a breach in respect of even a single person can be serious if the data is particularly sensitive. It does not follow that every data breach will always give rise to a potential claim, even if harm is caused. A claim for loss or distress may only be brought where it was caused by a contravention of the law by the School: for example if its data security was inadequate or an employee's unlawful actions were to blame.

What about breaches caused, or suffered, by our suppliers?
You may be liable for breaches affecting your own data which impact your suppliers, notably IT providers, which is one of the reasons it is important to have a robust contract in place. By law they must notify you "without undue delay" if they become aware first, but the contract should ideally

include a specified period. Any obligation on you to report begins once you are first made aware but the first hours and days are vital to minimising the impact.

What is the practical approach to dealing with a data breach?
A distinction ought to be drawn between an obviously serious breach that triggers a crisis plan (involving potential roles for IT, legal and PR advisers) and a more mundane breach that ought nevertheless to be dealt with as a matter of policy and record. Of course, it can be hard to see the difference before an assessment has taken place.
A step-by-step guide is provided on the next page (but this is a guide, rather than a substitute for a formal plan).

What does the ICO's Guidance say?
The ICO has an expanded section on data breach in its general Guide to the GDPR which is helpful.

The ICO's fuller guidance on data breach management has not been updated for GDPR. It still contains some valuable insights but its emphasis on assessment before notification will bring risks after 25 May 2018. The four elements that it identifies to breach management (1. Containment and recovery; 2. Assessment of ongoing risk; 3. Notification of breach; 4. Evaluation and response) remain relevant but should not be taken as a strict order of proceedings. From 25 May the recommendation must be for early notification, potentially on a provisional holding basis. GDPR allows for phased provision of information, so this may be followed up later (without undue delay) with either (a) fuller updates; or (b) confirmation that the matter is closed and contained without likely harm.

This means that neither the ICO's existing breach self-reporting form (which is quite detailed and requires filling out with care) nor malicious breach form (which is slightly less exacting) are likely to be suitable for every early notification. The ICO is setting up a telephone reporting line to sit alongside its online forms and it is to be hoped these will allow for provisional notifications and not be too prescriptive in terms of required fields. In any event Schools may wish to prepare their own forms to record internal assessments. Time will tell whether the ICO will accept these as valid reporting tools but they will have value as internal records (as required by GDPR).

What steps should we take to prevent data breaches?
There are two elements to this question: the "before" and "after". Plenty of sensible steps can be recommended to mitigate the likelihood, and likely impact, of future breaches. However, the risk of a breach can never be eliminated – whether due to sophisticated attacks, human error, or rogue employees – so learning to react is also critical. Your School's crisis management and/or business continuity plans should cover major breach incidents but having a data breach specific response plan (with allocated staff) is now on the ICO's GDPR checklist.

(a) Preparatory steps

On top of the crisis plan mentioned above, there is also routine best practice. In terms of basic data security groundwork, making sure School mobile devices and memory sticks are fully encrypted is an easy win. This should be tied in with effective policies on working from home, "bring your own device" protocols, email usage, data retention and secure deletion, information sharing and secure delivery methods and a meaningful password culture (including managing internal access rights to information which should be on a need-to-know basis).

Policy and structure is just as important as having secure IT. If a breach occurs, Schools will be expected to prove that staff training took place and policies were properly notified and enforced. Where Schools outsource systems and processes which require use of e.g. pupil data (which again goes beyond IT), they have a legal obligation to secure sufficient contractual guarantees that the data will be handled safely and by competent people.

(b) Remedial steps

Action after the event is also important: policy and systems review, re-training, and – for more major incidents – a review of the causes if the incident and the effectiveness of the School's response.

This is not simply a case of shutting the stable door: nothing improves practices like learning from mistakes and there will be future data incidents. From the ICO's perspective, a key aspect of closing a data breach case is noting the remedial steps taken: and, ideally, Schools will be pro-active in telling the ICO what they have done, rather than waiting to be told. When the next incident happens (as it inevitably will) the ICO will look at the School's past record and assess whether lessons were learned and whether any promises made were kept.

Subject Access Request Guidance

What is a "Subject Access right" (SAR)?

Both the Data Protection Act 1998 (DPA) and, from 25 May 2018, the General Data Protection Regulation (GDPR) provide for a right enjoyed by all individuals – including parents, pupils, staff (past, present and prospective) – 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.
Please note that the SAR is not the same as a parent's statutory right to receive a copy of their child's educational record under the Education Act 1996, which is sometimes cited by parents but does not apply to independent schools.

Why should we be concerned?

The definition of personal data is wide and includes correspondence, emails, minutes, reports, results, databases, lists and expressions of opinion. Given that independent schools have close relationships with pupils and parents, a good deal of personal data of this kind will be accumulated over the career of a pupil. Usually, individuals are also entitled to a "permanent copy" of the personal data held. In practice, this involves considerable effort, and can sometimes result in delicate or embarrassing disclosures and difficult decisions around the application of appropriate exceptions. Only repetitious requests, without allowing a reasonable time since the previous SAR, can safely be ignored.

The SAR right is wide in scope and has no time limitation. Schools can expect to incur considerable time and costs in responding fully, and – from 25 May 2018 – will no longer be able to charge even a token fee, except in limited cases.
What are the formalities need for making – or recognising – a valid SAR?

Very few: a SAR must be made in writing, but does not have to mention the DPA or GDPR (or use any of the technical jargon of the law of personal data), provided it is clear the requester wishes to access information about themselves held by the school. It can be validly made to anyone in the organisation, including online, and the effect (and period for responding) is the same. Schools can however request any information they reasonably required to confirm the identity or authority of the requester, or in order to locate the data sought (if this is not immediately obvious, with e.g. CCTV footage), before responding. Schools can ask requesters to use a specific "form" but cannot insist on this.

Informal requests may be very narrow, in which case the school can consider it on its own terms (rather than assume a full SAR) but still need to be mindful of the SAR rules, including to take care around the information of others.

Can a SAR be made on another's behalf?

Yes, provided the school 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, and indeed 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 twelves). A child of any age can also ask a parent or third party to make a SAR on their behalf.

If there is any doubt, it will always be reasonable to request a direct or signed "authority" from the individual (e.g. the pupil). It is good policy to do this as a matter of course with parental requests about secondary school age pupils.

What are the time limits for compliance?

GDPR 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). It is recommended that the school does not delay in starting the process, and keeps the requester informed: it is shorter than the 40 calendar days under the DPA, which itself has often proved very tight for larger requests.
It is not a serious contravention of the law to take longer, but it is a technical breach and may be used to criticise the school. In general it is better to get the disclosure "right" than to hurry and risk failing to make proper redactions.

What needs to be searched? Can we be proportionate?

All electronic systems under the school's control, which may include personal devices or email accounts where used on school business (by e.g. peripatetic music teachers or Trustees), and any "filing system" as defined by the GDPR. There is some encouragement in recent case law to suggest searches may be subject to proportionate considerations and the GDPR suggests that "manifestly unfounded or excessive" requests can be ignored or fairly charged for.

Under the DPA, SARs included hard copy records only to the extent they were sufficiently well-organised to give easy access to specific information about an individual. The GDPR arguably tightens this rule, but we await ICO Guidance.

What information has to be disclosed?

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. An entire email chain will not always be personal data of someone mentioned in the subject line, for example.

Some requesters will expect full document disclosure of anything of interest to them, but do be mindful that very often this may relate to their complaint without relating to them personally: it could be merely factual or procedural.

What if the information identifies other people?

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. Schools need to be aware that under the current draft DPA 2018 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.

Real care needs to be taken in this area, as disclosure of information which also relates to a third party may be undesirable and may even give rise to a breach of confidence or data protection towards that other person.

Are there any other exemptions to the Subject Access right?

Yes. 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.

What are the consequences of non-compliance with a SAR?

The DPA is enforced by the Information Commissioner's Office (ICO) and the Courts. Individuals who are unsatisfied with an organisation's response to a SAR may complain to the ICO, which will generally investigate and (usually, having given the organisation a chance to state its case) give its view on whether the organisation has complied with the law. In some cases the ICO may simply ask the organisation informally to re-consider, with no further consequences (though it will keep a record of the matter, which could have an impact on how future complaints are dealt with). Individuals may also make an application to court to enforce the request, which is at the court's discretion and is of course more expensive for all involved.

Formal enforcement action is rarer, but the ICO can be unpredictable in taking sides: if the ICO makes a recommendation (including to disclose), schools are well advised to comply to avoid the ICO using its stricter powers.

Is there any formality to disclosing the data?

Strictly, it does not matter how the data is delivered as long as it is intelligible to the requester – it could be compiled in a table or single document or scanned or photocopied from originals and sent digitally or by hard copy. In practice, care must be taken to ensure it is delivered securely (with effective redactions). The best way to effect safe delivery is by agreeing a time and method with the requester. Post, even by recorded delivery, is less secure than a courier – which in turn is less secure than collecting or delivering in person. Ordinary email is less secure than an encrypted transfer, and so on. The suitability of delivery will depend on the sensitivity, volume and nature of the data. CCTV may require careful thought and offering to show the person footage on-site may be safer than sending out copies.

GDPR sets out additional information about data and rights for inclusion in the cover letter with the data. Care must be taken to get this right and use the letter to manage fairly the requester's expectations about what they are getting.

Where can we get more information?

The ICO has published extensive guidance on the Subject Access right (available on its website, www.ico.org.uk), and most recently updated its pre-GDPR "Subject Access Code of Practice" (also available on the website) in 2017.