KING EDWARD'S SCHOOL
POLICY DOCUMENT

Title: Data Protection Policy and Procedures

Policy Category	Internal
Status	Approved
Approved by	Governing Board
Current Author	TVA
Last Approved/Updated	June 2023
Frequency of Review	2 yrs
Date of Next Review	June 2025
Application	Whole School
Staff Responsibility	Bursar/Data Protection lead

Contents

DATA PROTECTION POLICY

Background

This policy is based on the template provided by the School's Data Protection Officer Judicium and supplemented by information from ISBA and details specific to King Edward's School, Bath (the School). It will be reviewed every two years and updated whenever necessary. Existing staff will be notified of any updates via email. The School may update this Policy from time to time.
Copies of this policy will be available on the School website, the staff VLE and during Staff Induction.

Data protection is an important legal compliance issue for the School. During the course of the School's activities it collects, stores and processes personal data (sometimes sensitive in nature) about staff, pupils, their parents, its contractors and other third parties (in a manner more fully detailed in the School's Privacy Notice). The School, as "data controller", is liable for the actions of its staff and Governors in how they handle data. It is therefore an area where all staff have a part to play in ensuring we comply with and are mindful of our legal obligations, whether that personal data handling is sensitive or routine.

Without fundamentally changing the principles of data protection law, and while providing some helpful new grounds for processing certain types of personal data, in most ways this new law has strengthened the rights of individuals and placed tougher compliance obligations on organisations including schools that handle personal information. The Information Commissioner's Office (ICO) is responsible for enforcing data protection law, will typically look into individuals' complaints routinely and without cost, and has various powers to take action for breaches of the law.

Introduction

The UK General Data Protection Regulation (UK GDPR) ensures a balance between an individual's rights to privacy and the lawful processing of personal data undertaken by organisations in the course of their business. It aims to protect the rights of individuals about whom data is obtained, stored, processed or supplied and requires that organisations take appropriate security measures against unauthorised access, alteration, disclosure or destruction of personal data.

The School will protect and maintain a balance between data protection rights in accordance with the UK GDPR. This policy sets out how we handle the personal data of our past, current and prospective pupils, parents, suppliers, employees, workers and other third parties.

This policy does not form part of any individual's terms and conditions of employment with the School and is not intended to have contractual effect. Changes to data protection legislation will be monitored and further amendments may be required to this policy in order to remain compliant with legal obligations.

All members of staff are required to familiarise themselves with its content and comply with the provisions contained in it. Breach of this policy will be treated as a disciplinary offence which may result in disciplinary action under the School's Disciplinary Policy and Procedure up to and including summary dismissal depending on the seriousness of the breach.

This policy meets the requirements of the:

- UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020
- Data Protection Act 2018 (DPA 2018)

Definitions

King Edward's School, Bath (the School)	King Edward's School, Bath including the Senior School, Junior School and Pre-Prep School
King Edward's School is a "data controller."	This means that we are responsible for deciding how we hold and use personal information about you. We are required under data protection legislation to notify you of the information contained in this Policy.
DPL Person responsible for data protection in the School	The School's Data Protection Lead (DPL) can be contacted as follows: Mrs Tracy Vaid. Extn 210 Email: dataprotection@kesbath.com
Data Protection Officer:	We have appointed a data protection officer (DPO) to oversee compliance with data protection. If you have any questions about how we handle your personal information which cannot be resolved by the DPL, then you can contact the DPO. Judicium Consulting Limited Address: 72 Cannon Street, London, EC4N 6AE Email: dataservices@judicium.com Web: www.judiciumeducation.co.uk
Personal data	Personal data is any information relating to an individual where the individual can be identified (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access.
Special category personal data and Criminal Offence data	Personal data revealing racial or ethnic origin, political opinions, religious beliefs, philosophical beliefs or trade union membership, Genetic and biometric data, Data concerning health, sex life or sexual orientation. Criminal offence data including criminal activity, allegations, investigations and proceedings.

Key data protection terms used in this data protection policy are:

- **Data controller** – a person or body that determines the purpose and means of the processing of personal data, and who is legally responsible for how it is used. For example, the School (including its governors) is a controller. An independent contractor who makes their own such decisions is also, separately, likely to be a data controller.
- **Data processor** – an organisation that processes personal data on behalf of a data controller, for example a payroll or IT provider or other supplier of services with whom personal data may be shared but who is not authorised to make any decisions about how it is used.
- **Personal data breach** – a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.
- **Processing** – virtually anything done with personal information, including obtaining or collecting it, structuring it, analysing it, storing it, sharing it internally or with third parties (including making it available to be viewed electronically or otherwise), altering it or deleting it.

Application of this policy

This policy sets out the School's expectations and procedures with respect to processing any personal data we collect from data subjects (including parents, pupils, employees, contractors and third parties).

Those who handle personal data as employees or governors of the School are obliged to comply with this policy when doing so. For employees, breaches of this policy may result in disciplinary action. Accidental breaches of the law or this policy in handling personal data will happen from time to time, for example by human error, and will not always be treated a disciplinary issue. However, failure to report breaches that pose significant risks to the School or individuals will be considered a serious matter.

Sharing personal data

In addition, this policy represents the standard of compliance expected of those who handle the School's personal data as contractors, whether they are acting as "data processors" on the School's behalf (in which case they will be subject to binding contractual terms) or as data controllers responsible for handling such personal data in their own right.

Where the School shares personal data with third party data controllers – which may range from other schools, to parents, to appropriate authorities, to casual workers and volunteers – each party will need a lawful basis to process that personal data, and will be expected to do so lawfully and with due regard to security and confidentiality, as set out in this policy. In some instances, the School will enter into an Information Sharing Agreement with third party – where this is necessary, it will be dealt with by the Data Protection Lead.

If you are a volunteer or contractor, you will be a data controller in your own right, but the same legal regime and best practice standards set out in this policy will apply to you by law.

We will not normally share personal data with anyone else without consent, but there are certain circumstances where we may be required to do so. These include, but are not limited to, situations where:

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk
- We need to liaise with other agencies – we will seek consent as necessary before doing this
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies. When doing this, we will:
    - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with UK data protection law
    - Establish a contract with the supplier or contractor to ensure the fair and lawful processing of any personal data we share
    - Only share data that the supplier or contractor needs to carry out their service

We will also share personal data with law enforcement and government bodies where we are legally required to do so.

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils or staff.

Where we transfer personal data internationally, we will do so in accordance with UK data protection law.

The 7 Principles of UK General Data Protection Regulations

The GDPR sets out seven principles relating to the processing of personal data which must be adhered to by data controllers (and data processors). These require that personal data must be:

1) Processed **lawfully, fairly** and in a **transparent** manner; See Section below for detail of the lawful grounds for data processing
2) Collected for **specific and explicit purposes** and only for the purposes it was collected for;
3) **Relevant** and **limited** to what is necessary for the purposes it is processed;
4) Accurate and kept up to date;
5) **Kept for no longer than is necessary** for the purposes for which it is processed; and
6) Processed in a manner that ensures **appropriate security** of the personal data.
7) Accountability - The GDPR's broader 'accountability' principle also requires that the School not only processes personal data in a fair and legal manner but that we are also able to *demonstrate* that our processing is lawful. This involves, among other things:
    - keeping records of our data processing activities, including by way of logs and policies;
    - documenting significant decisions and assessments about how we use personal data (including via formal risk assessment documents called Data Protection Impact Assessments); and
    - generally having an 'audit trail' vis-à-vis data protection and privacy matters, including for example when and how our Privacy Notice(s) were updated; when staff training was undertaken; how and when any data protection consents were collected from individuals; how personal data breaches were dealt with, whether or not reported (and to whom), etc.

Lawful grounds for data processing

Under the GDPR there are several different lawful grounds for processing personal data. One of these is consent. However, because the definition of what constitutes consent has been tightened under GDPR (and the fact that it can be withdrawn by the data subject) it is considered preferable for the School to rely on another lawful ground where possible.

One of these alternative grounds is 'legitimate interests', which is the most flexible basis for processing. However, it does require transparency and a balancing assessment between the rights of the individual and the interests of the School. It can be challenged by data subjects and also means the School is taking on extra responsibility for considering and protecting people's rights and interests. The School's legitimate interests are set out in its Privacy Notice, as GDPR requires.

Other lawful grounds include:

- compliance with a legal obligation, including in connection with employment, engagement of services and diversity;
- contractual necessity, e.g. to perform a contract with staff or parents, or the engagement of contractors;
- a narrower set of grounds for processing special categories of personal data (such as health information), which includes explicit consent, emergencies, and specific public interest grounds.

Rights of Individuals

In addition to the School's responsibilities when processing personal data, individuals have certain specific rights, perhaps most significantly that of access to their personal data held by a data controller (i.e. the School).

If you receive a request from an individual who is purporting to exercise one or more of their data protection rights, you must tell the Data Protection Lead as soon as possible:

Extn 210

Email: dataprotection@kesbath.com

An individual has the following rights:

- **Right to be informed:** Individuals have the right to be informed about the collection and use of their personal data. This is a key transparency requirement under the UK GDPR. The School must provide individuals with information including: our purposes for processing their personal data, our retention periods for that personal data, and who it will be shared with. We call this 'privacy information'.
- **Right of access** : to obtain access to, and copies of, the personal data that we hold about you; This is known as the 'data subject access right' (or the right to make 'data subject access requests'). Such a request must be dealt with promptly and does not need any formality, nor to refer to the correct legislation
- **Right of rectification:** to require us to correct the personal data we hold about you if it is incorrect;
- **Right to erasure:** to require us (in certain circumstances) to erase your personal data;
- **Right to restrict processing:** to request that we restrict our data processing activities (and, where our processing is based on your consent, you may withdraw that consent, without affecting the lawfulness of our processing based on consent before its withdrawal);
- **Right to data portability:** to receive from us the personal data we hold about you which you have provided to us, in a reasonable format specified by you, including for the purpose of you transmitting that personal data to another data controller;
- **Right to object:** to object, on grounds relating to your particular situation, to any of our particular processing activities where you feel this has a disproportionate impact on your rights.

None of the above rights for individuals are unqualified and exceptions may well apply. However, certain rights are absolute and must be respected, specifically the right to:

- object to automated individual decision-making, including profiling (i.e. where a significant decision is made about the individual without human intervention)
- object to direct marketing
- withdraw one's consent where we are relying on it for processing their personal data (without affecting the lawfulness of processing carried out prior to that point in reliance on consent, or of any processing carried out on some other legal basis other than consent).

Children and subject access requests

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent.

Children aged 12 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests

from parents or carers of pupils at our school may not be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

Headline responsibilities of all staff

It is in everyone's interests to get data protection right and to think carefully about data protection issues: this means handling all personal information with which you come into contact fairly, lawfully, securely and responsibly.

All staff must read and sign the School's Acceptable Use Policy which sets out the rules for access to data and ICT systems.

A good rule of thumb here is to ask yourself questions such as:

- Would I be happy if my own personal information were being used (for example, shared with a third party) in the way I am proposing? Would I expect it?
- Would I wish to stand by how I have recorded this information in an email or official record if the person concerned were able to see it?
- What would be the consequences of my losing or misdirecting this personal data?

Simple guidelines to ensure a culture of data privacy in KES

Data protection law is best seen as a code of useful and sensible checks and balances to improve how we handle and record personal information and manage our relationships with people. This is an important part of the School's culture and all its staff and representatives need to be mindful of it.

A culture of Data Privacy in our School means that you:

1. Keep personal data private and secure
2. Delete personal data you don't need to keep
3. Know what you are using the data for and how long you will keep it
4. Ensure you have the relevant permissions before sharing personal data and alert subjects to their rights using our privacy notices
5. Should you receive data requests pass them on to your line manager/DPL straight away
6. Don't take personal data home or transfer data onto personal devices

Record-keeping

It is important that personal data held by the School is accurate, fair and adequate. Staff are required to inform the School if they believe that any personal data is inaccurate or untrue or if you are dissatisfied with how it is recorded. This applies to how staff record their own data, and the personal data of others – colleagues, pupils and their parents – in a way that is professional and appropriate.

Staff should be aware of an individual's rights with regard to their data, whereby any individuals about whom they record information on School business (notably in emails and notes) digitally or in hard copy files may have the right to see that information. This absolutely must not discourage staff from recording necessary and sometimes difficult records of incidents or conversations involving colleagues or pupils, in accordance with the School's other policies, and grounds may sometimes exist to withhold these from such requests. **However, the starting position for staff is to record every document or email in a form they would be prepared to stand by should the person about whom it was recorded ask to see it.**

The Table of Retention Periods (attached) lists the amount of time the School will retain personal data gathered.

Data handling

All staff have a responsibility to handle the personal data which they encounter fairly, lawfully, responsibly and securely and in accordance with the staff handbook and all relevant School policies and procedures (to the extent applicable to them). There are data protection implications across several areas of the School's wider responsibilities such as safeguarding and IT security, so all staff should read and comply with the following policies:

- Safeguarding & Child Protection (KCSIE)
- Acceptable Use

Responsible processing also extends to the creation and generation of new personal data/records, as above, which should always be done fairly, lawfully, responsibly and securely.

Care and data security

More generally, we require all School staff (and expect all our contractors) to remain mindful of the data protection principles (see section above), and to use their best efforts to comply with those principles whenever they process personal information. Data security is not simply an online or digital issue but one that effects daily processes: filing and sending correspondence, notably hard copy documents. Data handlers should always consider what they most assured and secure means of delivery is, and what the consequences would be of loss or unauthorised access.

We expect all those with management / leadership responsibilities to be particular champions of these principles and to oversee the swift reporting of any concerns about how personal information is used by the School.

Data Security: online and digital

The School must ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data.

- No member of staff should provide personal data of pupils or parents to third parties, including a volunteer or contractor, unless there is a lawful reason to do so and a signed Information Sharing Agreement is in place (where appropriate).
- Use of personal email accounts or unencrypted personal devices by staff for official School business is not permitted.

Only full disk encryption solutions approved by IT Support and configured according to standards set by IT Support may be utilized to satisfy the requirements of this policy. The encryption solution (End Point Manager) will centrally manage the full disk encryption client software for all systems, including encryption format, key management, and logging. IT Support will centrally maintain copies of encryption keys and encryption audit logs. King Edward's School retains the right to decrypt data using the centrally maintained key as required.

Users must report any known, unencrypted personal information on portable computing devices to IT Support and request assistance in removing the data or securing it.

It is a violation of this policy for anyone to attempt to disable, remove, or otherwise tamper with the encryption software. Failure to comply with this policy regarding the encryption of Personal Information may result in disciplinary action up to and including termination of employment.

Processing of Financial / Credit Card Data

The School complies with the requirements of the PCI Data Security Standard (PCI DSS). Staff who are required to process credit card data must ensure that they are aware of and comply with the most up to date PCI DSS requirements. If you are unsure in this regard, please seek further guidance from the Bursar. Other categories of financial information, including bank details and salary, or information commonly used in identity theft (such as national insurance numbers or passport details), may not be treated as legally sensitive but can have material impact on individuals and should be handled accordingly.

Photographs and videos

As part of our school activities, we may take photographs and record images of individuals within our school.

We do not allow any photos or videos to be taken of pupils by third parties during a visit to the School. We routinely take photos of events hosted or run by third parties and share these on the School's website and social media platforms. Visiting organisations or individuals are encouraged to share these posts as a way of referencing their visit. If an organisation would like to use a photo on its website, please speak to the School's Marketing Team. In these situations, we will endeavour to select an appropriate image and ensure that the required approvals are in place for use on third party websites for a specified period of time.

See our Child protection and Safeguarding policy for more information on our use of photographs and videos.

Data protection by design and default

We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Appointing a suitably qualified DPO and DPL and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge

- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law
- Completing data protection impact assessments where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPL will advise on this process)
- Integrating data protection into internal documents including this policy, and related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance/completion of this training
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Appropriate safeguards being put in place if we transfer any personal data outside of the UK, where different data protection laws may apply
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our school and DPO, and all information we are required to share about how we use and process their personal data (via our privacy notices)
    - For all personal data that we hold, maintaining an internal record of the type of data, type of data subject, how and why we are using the data, any third-party recipients, any transfers outside of the UK and the safeguards for those, retention periods and how we are keeping the data secure

Data security and storage of records

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

In particular:

Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, or left anywhere else where there is general access

Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected

See our Staff Acceptable Use policy for more information.

Disposal of records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law. See Table of Retention Periods in Appendix 3 for further details.

Avoiding, mitigating and reporting data breaches

A personal data breach includes, but is not restricted to, the following:

• Attempts (either failed or successful) to gain unauthorised access to a system or its data
• Unwanted disruption or denial of service
• The unauthorised use of a system for the processing or storage of data
• Changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent
• Loss of removable media (USB stick, disc etc) and portable equipment (laptops/tablet PCs)
• Tampering/attempting to tamper with CCTV cameras or the leaking of unauthorised film footage taken from CCTV equipment
• Damage to or theft /loss of ICT equipment or confidential / sensitive papers (either manual or electronic)
• Unauthorised access to confidential / sensitive information in any form including receiving information meant for someone else
• Unauthorised disclosure of confidential / sensitive information in any form to a third party
• Transfer of information to the wrong person (by fax, email, post or phone)
• The finding of confidential information/records in a public area
• The unauthorised usage of another user's security credentials
• Sharing computer ID and passwords
• Accessing another individual's personal details without permission.
• Leaving confidential / sensitive information on public display
• Virus outbreak.

Data controllers must report certain types of personal data breach (those which risk an impact to individuals) to the ICO within 72 hours. In addition, data controllers must notify individuals affected if the breach is likely to result in a "high risk" to their rights and freedoms. The School must keep a record of any personal data breaches, regardless of whether we need to notify the ICO.

For the purposes of this policy data security breaches include both confirmed and suspected incidents.

The following must be considered upon discovering a data breach:

- The type of data involved
- Its sensitivity
- If data has been lost or stolen, whether data has been protected by encrypted devices or software
- What has happened to the data, such as the possibility that it may be used to cause harm to an individual
- Who the individuals are, number of individuals involved and the potential effects to those data subjects
- Whether there are wider consequences to the breach
- Whether any actions have been taken during the breach that contravene the policies, procedures and training in place.

If staff are in any doubt as to whether to report something internally, it is always best to do so using the procedure in Appendix 1.

A personal data breach may be serious, or it may be minor; and it may involve fault or not; but the School always needs to know about them to make a decision.

As stated above, the School may not need to treat the incident itself as a disciplinary matter – but a failure to report could result in significant exposure for the School, and for those affected,

and could be a serious disciplinary matter whether under this policy or the applicable staff member's contract.

Training

All Staff must attend or undertake any training we require them to on a regular basis.

Appendix 1: Personal data breach procedure

This procedure is based on guidance on personal data breaches produced by the Information Commissioner's Office (ICO).

Every care is taken by the School to protect personal data from situations where a data protection breach could compromise security.

This policy and procedure applies to all staff, students, parents, Governors, employees, suppliers or third parties we work with.

The objective of this policy is to enable staff to act promptly to contain any breaches that occur, minimising the risk associated with the breach and to take action if necessary to secure personal data and prevent further breaches.

The School expects its staff to embed security and prevention practices in their normal working day to ensure personal, or special category, data is protected for the purposes of school business and must take appropriate steps to safeguard this information.

Under the Data Protection Act, although there is no legal obligation on data controllers to report breaches of security, the new General Data Protection Regulation (GDPR) means we have to report any breach that is likely to impact on data subjects. The procedure below is set out to help you identify when a breach has taken place and what the action should be.

On finding or causing a breach or potential breach, the staff member, governor or data processor must immediately notify the data protection lead (DPL)

Extn 210

Email: dataprotection@kesbath.com

The DPL will investigate the report and determine whether a breach has occurred. To decide, the DPL will consider whether personal data has been accidentally or unlawfully:

- Lost / Stolen
- Destroyed
- Altered
- Disclosed or made available where it should not have been
- Made available to unauthorised people

Staff and governors will co-operate with the investigation (including allowing access to information).

The DPL will make all reasonable efforts to contain and minimise the impact of the breach. Relevant staff members or data processors should help the DPL with this where necessary, and the DPL should take external advice when required (e.g. from IT providers).

The DPL will assess the potential consequences (based on how serious they are and how likely they are to happen) before and after the implementation of steps to mitigate the consequences- the DPL will seek advice from the DPO where necessary.

The DPL will work out whether the breach must be reported to the ICO and the individuals affected using the ICO's self-assessment tool and advice from the DPO.

The DPO will document the decisions (either way), in case the decisions are challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored in the Data breach Register.

Where the ICO must be notified, the DPL will send the relevant information to the DPO who will complete the report and liaise with the ICO on the School's behalf. The DPO will do this via the 'report a breach' page of the ICO website, or through its breach report line (0303 123 1113), within 72 hours of the school's awareness of the breach. As required, the DPO will set out:

- A description of the nature of the personal data breach including, where possible:
- The categories and approximate number of individuals concerned
- The categories and approximate number of personal data records concerned
- The name and contact details of the DPO
- A description of the likely consequences of the personal data breach
- A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned

If all the above details are not yet known, the DPO will report as much as they can within 72 hours of the school's awareness of the breach. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible.

Where the school is required to communicate with individuals whose personal data has been breached, the DPO will tell them in writing. This notification will set out:

- A description, in clear and plain language, of the nature of the personal data breach
- The name and contact details of the DPO
- A description of the likely consequences of the personal data breach
- A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned

The DPO will consider, in light of the investigation and any engagement with affected individuals, whether to notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies.

The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:

- Facts and cause
- Effects
- Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

Records of all breaches will be kept in a log on a secure GDPR folder accessible to the DPL and Senior Staff and reportable breaches are reported to the Governing Board termly.

The DPL and Bursar will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible

The DPL and Bursar will meet regularly to assess recorded data breaches and identify any trends or patterns requiring action by the school to reduce risks of future breaches

Appendix 2: Data Subject Access Request procedure

A data subject (anyone about whom we store personal data) can request access to the data we hold on them at ANY time

If you believe you have received a Data Subject Access Request (DSAR) you must immediately notify the data protection lead (DPL)

Extn 210

Email: dataprotection@kesbath.com

- Anyone can receive a DSAR at any time
- It can come in any form ie written email, letter or phone etc and does not necessarily contain the reference to DSAR.
- There is a very strict one calendar month reply timescale for responses
- DSAR's are managed centrally by the DPL to ensure authorised access to all personal data, confidentiality and compliance with legislation is maintained.

Appendix 3: Table of Retention Periods

Type of Record/Document	**Retention Period** Records will be kept beyond the suggested retention period where there is a legal obligation to retain the records for a longer period.
SCHOOL-SPECIFIC RECORDS	
• Registration documents of the School	Permanent (or until closure of the School)
• Attendance Register	6 years from last date of entry, then archive.
• Minutes of Governors' meetings	Permanent
• Annual curriculum	From end of year: 3 years (or 1 year for other class records: eg marks / timetables / assignments)
• Complaints	Records of complaints retained for a minimum of 25 years from the date the School becomes aware.
INDIVIDUAL PUPIL RECORDS	*These records contain personal data*
• Admissions: application forms, assessments, records of decisions	25 years from date of birth, or if pupil not admitted, up to 7 years from decision. 7 years from pupil leaving school and then passed to Archive.
• Pupil file including pupil reports, examination results (external or internal) and pupil performance records	25 years from date of birth and then archived (see section 11), subject where relevant to safeguarding considerations. Any material that may be relevant to potential claims will be kept for the lifetime of the pupil.
• Pupil medical records	25 years from date of birth, subject where relevant to safeguarding considerations. Any material that may be relevant to potential claims should be kept for the lifetime of the pupil.
• Special educational needs records (to be risk assessed individually)	25 years from date of birth, subject where relevant to safeguarding considerations. Any material that may be relevant to potential claims should be kept for the lifetime of the pupil.

• Copies of school bills	7 years after issue
SAFEGUARDING • Policies and procedures	Keep a permanent record of historic policies
• DBS disclosure certificates (potentially sensitive personal data & must be secure)	No longer than 6 months from decision on recruitment, unless DBS specifically consulted but maintain a record of the fact that checks were undertaken, if not the certificate itself. *These records contain personal and sensitive data.*
• Incident reporting	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.
• Safeguarding/Child Protection Files (including where a pupil has transferred to another school)	If a referral has been made / social care have been involved or child has been made subject of a multi-agency plan – indefinitely. If low level concerns, with no multi-agency action, assess at 25 years from date School becomes aware of incident or keep indefinitely, dependent on the concern.
CORPORATE RECORDS (where applicable) • Certificates of Incorporation	Permanent (or until dissolution of the company).
• Minutes, Notes and Resolutions of Boards or Management Meetings	Permanent
• Shareholder resolutions	Permanent
• Register of Members/Shareholders	Permanent (minimum 10 years for ex-members/shareholders).
• Annual reports	Permanent

ACCOUNTING RECORDS[3] • 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)	7 years from the end of the financial year in which the transaction took place.
• Tax returns	7 years
• VAT returns	7 years
• Budget and internal financial reports	3 years
CONTRACTS AND AGREEMENTS • Signed or final/concluded agreements (plus any signed or final/concluded variations or amendments)	7 years from completion of contractual obligations or term of agreement, whichever is the later.
• Deeds (or contracts under seal)	13 years from completion of contractual obligation or term of agreement.
INTELLECTUAL PROPERTY RECORDS • Formal documents of title (trademark or registered design certificates; patent or utility model certificates)	Permanent (in the case of any right which can be permanently extended, eg trade marks); otherwise expiry of right plus minimum of 7 years.
• Assignments of intellectual property to or from the school	As above in relation to contracts (7 years) or, where applicable, deeds (13 years).
• IP / IT agreements (including software licences and ancillary agreements eg maintenance; storage; development; co-existence agreements; consents)	7 years from completion of contractual obligation concerned or term of agreement.

EMPLOYEE / PERSONNEL RECORDS • Single Central Record of employees	*These records contain personal data* Keep a permanent record (not DBS certificates) of all mandatory checks that have been undertaken.
• Contracts of employment	7 years from effective date of end of contract.
• Employee appraisals or reviews • Staff Personnel File	7 years from effective date of end of contract. All staff HR files to be kept for the duration of any IICSA after which the School will follow guidance from the relevant authorities. Currently this stands at normal pension age, or for 10 years if longer. The School is required to keep records of complaints or concerns for a minimum of 25 years from the date the School became aware.
• Payroll, salary, maternity pay records	6 years
• Pension or other benefit schedule records	Teachers' Pension returns - permanent Pension schemes via payroll - 7 years
• Job application and interview/rejection records (unsuccessful applicants)	1 year (see note of DBS disclosure certificates).
• Immigration records	4 years
• Health records relating to employees	7 years from end of contract of employment.
INSURANCE RECORDS • Insurance policies (will vary - private, public, professional indemnity)	Permanent
• Correspondence related to claims/ renewals/ notification re: insurance	7 years

ENVIRONMENTAL & HEALTH RECORDS[1] • Maintenance logs • Accidents to children	10 years from date of last entry 25 years from birth (unless a safeguarding incident - see safeguarding section)
• Accident at work records (staff)	4 years from date of accident but review case by case if possible
• Staff use of hazardous substances • Risk assessments (carried out in respect of above)	7 years from end of date of use. 7 years from completion of relevant project, incident, event or activity.

[1] The School is aware that latent injuries can take years to manifest, and the limitation period for claims reflects this. The School will keep a note of all procedures as they were at the time, a record that they were followed and the relevant insurance documents