KNIGHTSBRIDGE
SCHOOL

Knightsbridge School Data Protection Policy

Knightsbridge School collects, stores and processes a wide range of data including information relating to pupils, parents/guardians, staff, contractors, suppliers and other professional contacts (collectively, "**data subjects**") and much of this data is personal in nature. Consequently the school is subject to the current data protection laws effective in the UK - the EU General Data Protection Regulation (GDPR) of 28 May 2018 and the UK Data Protection Act 2018. In the UK these legal obligations are overseen by the Information Commissioner's Office (ICO) where for the purposes of data protection, the school is classified as a "**data controller**". As data controller the school determines the purposes for, and means of processing personal data. The legislation also covers the activities of "**data processors**", and in this context they are any third party that processes personal data on behalf of the school.

UK data protection law applies to the processing of 'personal data', meaning the processing of any personal information relating to an individual, who can be directly or indirectly identified as a result. Further, some of the personal information handled by the school is classed as "special category data" that is personal data that is more sensitive in nature and so is subject to additional measures and controls.

This policy sets out Knightsbridge School's rules and guidelines for understanding and handling the personal data of its data subjects and how this fits within current legislation. The handling of personal data is likely something that all staff will be required to do in some way as part of their normal duties and so every member of staff must comply with this policy, whether the personal data in question is sensitive or not. Some members of staff, especially those in school management, administration, safeguarding, HR & IT handle greater volumes of, or more sensitive personal data and so these roles have additional responsibilities that require a more comprehensive understanding of data protection law, the measures put in place to ensure personal data is protected and the rights of data subjects. While we acknowledge accidental data breaches can happen and they may not be a disciplinary issue, breaches of this policy can result in disciplinary action.

Principles of Data Protection

As data controller the school is obliged to ensure personal data is:

1. Processed lawfully, fairly and in a transparent manner in relation to data subjects

2. Only used for the reasons it is collected and not for something extra or unrelated
3. Limited to only what is necessary for the purposes for which it is processed
4. Accurate and kept up to date
5. Only kept for as long as it is needed and when it is no longer needed it will be securely destroyed or deleted
6. Kept securely while maintaining appropriate access to only those that need it and is protected against unauthorised or unlawful processing, accidental loss, destruction or damage
7. Managed with accountability. The school takes responsibility for having appropriate measures in place, and keeps records to demonstrate data protection compliance.

These principles of UK data protection law require the school to provide data privacy notices that give data subjects information about the personal data processing activities, the legal basis of processing and their data subject rights. In order to demonstrate compliance the law also requires the school to maintain a policy for the handling of special category data, reporting a data breach, managing data subject access requests, data retention and to provide regular data protection training for staff.

The School Data Protection Lead

While not obliged to appoint a Data Protection Officer the school has a Data Protection Lead who will be the school's representative and ensure that all personal data is processed in compliance with this policy and the principles of current data protection legislation. The Data Protection Lead will be the point of contact for all questions about the operation of this policy, changes to what is, or the way personal data is processed, suspected data breaches and for raising any concern that the policy has not been followed. The Data Protection Lead is also responsible for coordinating the response to a suspected data breach that is aligned with policy, communicating and reporting to school leadership, the ICO and the police if necessary. In addition the Data Protection Lead is responsible for regular ongoing review of data protection practices and procedures including identifying the need for and delivering staff data protection training.

Lawful grounds for data processing

As a data controller the school needs to make clear the legal basis for processing personal data. In many cases this is **'legitimate interest'** i.e. for the legitimate

interest of the school to provide a safe and inclusive environment to educate its pupils. This specific ground for data processing requires transparency and the data controller to balance the rights of the data subject with their own interests as a school. It can be challenged by data subjects and it also means the data controller is taking on extra responsibility for considering and protecting other people's rights and interests.

The other lawful grounds are:

- '**Legal obligation**' - the processing is necessary for the school to comply with the law, including processing in connection with safeguarding, employment and diversity
- '**Contract**' - to fulfil a contract between the school and a person
- '**Vital interests**' - the processing is necessary to protect someone's life
- '**Consent**' - a person has given clear consent for the school to process their personal data for a specific purpose
- '**Public task**' - the processing is necessary for the school to perform a task in the public interest or for its official functions, and the task or function has a clear basis in law.

The schools legitimate interests and any other grounds for specific processing activities are set out in the Data Privacy Notices.

Rights of individuals - Subject Access Requests

In addition to the school's responsibilities when processing personal data, individual data subjects have certain rights, most significantly that of access to their personal data held by the school. This is known as the 'subject access right' or the right to make 'subject access requests'. Such a request must be dealt with promptly and does not need any formality, nor to refer to the correct legislation. If you become aware of a subject access request (or indeed any communication from an individual about their personal data), you must follow the Subject Access Request Policy and inform the Data Protection Lead without delay.

Individuals also have legal rights to:

- Require us to correct the personal data we hold about them if it is inaccurate
- Request that we erase their personal data (in certain circumstances)
- Request that we restrict our data processing activities (in certain circumstances)
- Receive from us the personal data we hold about them for the purpose of transmitting it in a commonly used format to another data controller
- Object, on grounds relating to their particular situation, to any of our particular

processing activities where the individual feels this has a disproportionate impact on them; and

- Object to any automated individual decision-making, including profiling (where a significant decision is made about the individual without human intervention)
- Withdraw their consent where we are relying on it for processing their personal data (e.g. for marketing purposes)

Except for the final point above, none of these rights for individuals are unqualified and exceptions may well apply. In any event, however, 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 without delay.

Key responsibilities for all staff

1. Record-keeping

It is important that personal data held by the School is accurate, fair and adequate. You are encouraged to inform the School if you believe that your or someone else's personal data is inaccurate, incomplete, untrue or if you are concerned with the information in any way. It is vital that whenever you record the personal data of others, such as colleagues, pupils and their parents/guardians, it is accurate, professional and appropriate.

Staff should be aware of the rights of data subjects to access information about them extends to email and messages exchanged on school systems. 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; nor does it ever endorse the use of personal accounts for this purpose. Rather, the starting position is to record every document or email in such a way that you are able to stand by what you have written if the person it concerns were to read it.

2. Data handling

All staff have a responsibility to handle the personal data which they come into contact with fairly, lawfully, responsibly and securely and in accordance with all relevant school policies and procedures. In particular, there are data protection implications across a number of areas of the School's wider responsibilities, so in addition to this policy all staff should be versed in the following:

- Data Privacy Notices

- Safeguarding Child Protection Policy
- CCTV Policy
- Remote Learning & Distance Teaching & Learning Guidances
- IT & E-Safety Policy
- IT Acceptable Use
- Code of Conduct

Responsible processing also extends to the creation and generation of new personal data / records and in addition staff should consider whether there is an existing lawful basis for the processing or whether a new lawful basis should be sought and recorded in the appropriate data privacy notice(s).

3. Reporting data breaches

Data controllers must report any data breach that risks an impact to individuals rights or freedom to the ICO within 72 hours of the breach being discovered. In addition, data controllers must also notify the individuals affected if the breach is likely to result in a "high risk" to their rights and freedoms.

In any event, the school must keep a record of any personal data breaches, regardless of whether we need to notify the ICO. If you become aware of a personal data breach you must follow the School's Data Breach Policy and notify the Data Protection Lead without delay. If you are in any doubt as to whether or not you should report an incident, it is always best to do so. 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 a breach in order to make the correct decisions.

The School may not need to treat the incident itself as a disciplinary matter, especially if policy has been followed, but a failure to report a breach could result in significant exposure for the school and for those individuals affected, and so it would be a disciplinary matter whether under this policy or the your employment or service contract.

4. Care for others personal data

More generally, we require all school staff to remain conscious of the data protection principles, to attend all training required, and to use their best efforts to comply with those principles whenever they process others' personal information. Data protection is not simply an online or digital issue but one that affects daily tasks such as filing and sending correspondence, including printed, hard copy documents; displaying notices and documents left on desks. Staff should always consider what personal information is being handled, the most assured and secure means of delivery for it is, and the consequences be for loss or unauthorised access.

We expect all those with management or leadership responsibilities to be well versed with these principles, to promote them when working with other staff and to oversee the swift reporting of any breaches or concerns about how personal information is used by the school to the Data Protection Lead, and to communicate any identified needs for additional staff training in this area.

5. Data Security - Digital, printed and online

All staff must ensure that they do not engage in unlawful or unauthorised processing of personal data, and be alert to the dangers of accidental loss, breach or damage to personal data. Therefore:

- With the exception of pupils' work, no member of staff is permitted to remove personal data from the school premises or school systems, whether in paper or electronic form and however stored, without prior consent
- Staff must ensure any personal data, including pupils' work, is stored securely and that it's never left unattended in transit whether on or off the school site
- The use of personal email, messaging, file sharing or other personal cloud accounts for official school business is not permitted
- The use of personal devices without both lock protection and encryption is not permitted for official school business
- Staff should never use external hard drives, memory sticks or personal cloud storage accounts to store or transfer data to or from school. The school provides secure services including Google Workspace for Education and the remote desktop access service that allow you to access data securely when on and off school site
- All staff must adopt a 'clear desk' approach to minimise the risk of personal data being left unattended on their desks
- Special care must be taken when sharing files, documents and digital media outside of the school organisation. Staff must consider what personal information is involved if any, whether special category data is included and how best to ensure it is shared appropriately. If ever in doubt, always defer advice from the Data Protection Lead or failing this, a member of Senior Management or the IT team
- Staff must always lock their computers or log out when away from their desk and lock screens on devices when left unattended
- For those handling special category personal data further precautions should be taken including locking their office doors when unattended and locking paper filing cabinets and drawers between accesses.

KNIGHTSBRIDGE
SCHOOL

Summary

It is in everyone's interests to get data protection right and to always have it at the forefront of our thinking. This means handling all personal information with which you come into contact fairly, lawfully, securely and responsibly. Good practice is to regularly 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 and have I agreed to it?
- Can I stand by what I have written in an email or official record if the person concerned was able to see it?
- How could the handling of this personal data lead to loss or inappropriate sharing?
- Is this the most appropriate way to handle, process or share this personal information?
- When looking to sign up or adopting a new web based service for your work at school - does the provider comply with UK GDPR? Do they act as a data processor or assume data controller rights? Have I followed the school's approval process for signing up to the account?
- How can I ensure the personal data I need to work with does not reside on my personal device or computer?

If you are ever in any doubt, always check first with the school Data Protect Lead.

Data protection law is a helpful set of checks and balances that improve how we record, handle and store personal information and manage our relationships with pupils, parents / guardians, colleagues and other professional contacts. It forms an important part of school culture and all school staff and representatives are required to follow it.

Prepared by: Simon Harrison (DPL) August 2023

Reviewed by: Shona Colaço (Head) August 2023

This policy will be reviewed annually or in the event of changes in legislation

KNIGHTSBRIDGE
SCHOOL

Appendix 1 - Data Privacy Notices

Data Privacy Notice for Parents and Pupils

(including prospective parents and pupils)

This privacy notice explains how Knightsbridge School collects and uses personal information about parents and pupils. We are the data controller for the personal information we collect about you.

The personal information we collect

- Medical information, such as your child's allergies and medical conditions
- Any special educational needs information for your child, if applicable
- Other information that you proviContact information, such as your name, address, email address, and phone number
- Demographic information, such as your child's age, gender, and ethnicity
- Education information, such as your child's academic records and attendance history
- de to us, such as your child's interests and extracurricular activities
- Financial information, such as your payment details for school fees
- Passport, visa and agent details, if relevant

How we collect personal information

- When you register your child for school
- When you communicate with us, such as when you send us an email or call us
- When your child attends school, such as when we take attendance or record their grades
- From other organisations, such as a previous school or a report from your child's doctor
- When your child participates in school activities
- When you make a payment for school fees

How we use personal information

- To provide education to your child

- To communicate with you about your child's education
- To manage your child's school records
- To provide medical care to your child, if necessary
- To protect the safety of your child and other pupils
- To provide your child with support for their special educational needs, if applicable
- To collect payments for school fees
- To comply with legal requirements

Who we share personal information with

We may share limited personal information about pupils and parents with the following third parties:

- Appropriate regulatory bodies e.g. the Independent Schools Inspectorate
- Government agencies, such as the Department for Education
- Health care providers
- Other organisations that provide services to your child, such as transport, caterers and clubs providers
- Local authorities
- Third-party services, such as IT providers
- Other schools or educational organisations

Legal basis for processing personal data

- Contractual necessity: We may process your personal data to fulfil our contractual obligations to you, such as providing your child with an education
- Legal obligation: We may process your personal data to comply with a legal obligation, such as maintaining school records
- Vital interests: We may process your personal data in the vital interests of your child, such as if they need medical care
- Legitimate interests: We may process your personal data in our legitimate interests, such as to improve our school services or to communicate our offerings to you and your child
- Consent: We may ask for your consent to process your personal data for certain purposes, such as marketing our school to other parents and celebrating our achievements amongst the wider community

KNIGHTSBRIDGE SCHOOL

How we protect personal information

We take steps to protect the security of personal information we collect about parents and pupils, including:

- Using appropriate technical and organisational measures to protect your data
- Regularly training staff in data protection and cyber security principles and requiring them to keep personal information confidential
- Encrypting personal information when it is transferred electronically
- Limiting access to your data to only authorised staff
- Keeping your data up to date
- Deleting your data when it is no longer needed or no longer required by law

How long we keep personal information

We will keep personal information about parents and pupils for as long as is necessary for the purposes for which it was collected, or as required by law.

Your rights

You have the following rights with respect to your personal information:

- The right to access your personal information
- The right to correct any inaccuracies in your personal information
- The right to request that we delete your personal information
- The right to object to our processing of your personal information
- The right to restrict our processing of your personal information
- The right to data portability
- The right to complain to the Information Commissioner's Office (ico.org.uk)

These rights are in some circumstances, dependent on the legal basis your information is being processed.

How to contact us

If you have any questions about this privacy notice, please contact the School Data Privacy Lead at:

Knightsbridge School
67 Pont Street, London, SW1X 0BD
020 7590 9000
dataprotection@knightsbridgeschool.com

Changes to this privacy notice

We may update this privacy notice from time to time. The latest version will always be available on request.

KNIGHTSBRIDGE
SCHOOL

Data Privacy Notice for School Staff

This privacy notice explains how Knightsbridge School collects and uses personal information about staff, including employees, peripatetic staff, consultants and contractors. We are the data controller for the personal information we collect about you.

The personal information we collect

- Contact details, such as name, address, email address, and phone number
- Employment details, such as job title, start date, and salary
- Personal characteristics, such as date of birth, gender, and ethnicity
- Education and training history
- References
- Criminal record checks
- Health records, if necessary for the performance of your job
- Ongoing appraisal records during the course of employment

How we collect personal information

- When you apply for a job with us
- When you are employed by us
- When you interact with us in the course of your employment
- From third parties, such as background check providers

Why we collect this personal information

- To manage your employment, such as paying your salary, providing you with benefits, and managing your performance
- To comply with legal obligations, such as health and safety regulations
- To provide you with training and development opportunities
- To assess your suitability for employment
- To contact you about school matters
- To protect the safety of our staff and pupils
- To improve the quality of the education and opportunities that we provide

KNIGHTSBRIDGE SCHOOL

Who we share personal information with

We may share limited personal information about pupils and parents with the following third parties:

- Our payroll provider
- IT service providers
- Other schools in our group
- Government agencies
- Professional bodies, such as our insurers & lawyers
- Training providers
- Medical professionals
- Background check providers
- Any other third parties who we are required to share your data with by law

The legal basis for processing your personal information

- Contract: We need to process your personal data to perform our contract with you, such as to pay you your salary and provide you with benefits
- Legal obligation: We need to process your personal data to comply with legal obligations, such as to keep records of your employment
- Legitimate interests: We may also process your personal data on the basis of our legitimate interests, such as to protect the safety of our staff and pupils; to improve our school services or to communicate with parents and pupils
- Consent: We may ask for your consent to process your personal data for certain purposes, such as marketing the school and celebrating our achievements amongst the wider community

How we protect your personal information

- We use appropriate technical and organisational measures to protect your data
- We regularly train you in data protection and cyber security principles and we require you to keep your own and others personal information confidential
- We encrypt personal information when it is transferred electronically
- We limit access to your data to only authorised staff
- We keep your data up to date
- We delete your data when it is no longer needed or no longer required by law

KNIGHTSBRIDGE
SCHOOL

How long we keep your personal information

We will keep your personal data for as long as is necessary for the purposes for which we collected it, or as required by law.

Your rights

You have the following rights with respect to your personal information:

- The right to access your personal information
- The right to correct any inaccuracies in your personal information
- The right to request that we delete your personal information
- The right to object to our processing of your personal information
- The right to restrict our processing of your personal information
- The right to data portability
- The right to complain to the Information Commissioner's Office (ico.org.uk)

These rights are in some circumstances, dependent on the legal basis your information is being processed.

How to contact us

If you have any questions about this privacy notice, please contact the School Data Privacy Lead at:

Knightsbridge School
67 Pont Street, London, SW1X 0BD
020 7590 9000
dataprotection@knightsbridgeschool.com

Changes to this privacy notice

We may update this privacy notice from time to time. The latest version will always be available on request.

KNIGHTSBRIDGE
SCHOOL

Appendix 2 - Special Category Data Policy

This policy sets out how Knightsbridge School processes special category data. Special category data is personal data that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, or data concerning a natural person's sex life or sexual orientation.

Purpose of processing

We will only process special category data for the following purposes:

- To provide education and care to our pupils
- To comply with legal obligations, such as the Equality Act 2010, DfE Census, pupil counselling and safeguarding children
- To protect the safety of our pupils and staff
- To prevent fraud and other crime
- To monitor and improve our services

Legal basis for processing

- Legal obligation: We may process special category data if we are required to do so by law, such as the Equality Act 2010.
- Vital interests: We may process special category data if it is necessary to protect the vital interests of you or another person.
- Public interest: We may process special category data if it is necessary in the public interest, such as for the prevention of crime.
- Legitimate interests: We may process special category data if it is necessary for our legitimate interests, such as to provide education and care to our pupils.
- Explicit consent: We will obtain your explicit consent before processing special category data about you, unless we are able to rely on another legal basis.

Data sharing

We will only share special category data with third parties where it is necessary for the purpose for which it was collected, or where we are legally required to do so.

Data security

We will take all reasonable steps to protect special category data from unauthorised access, disclosure, alteration, or destruction.

Data retention

We will only retain special category data for as long as is necessary for the purpose for which it was collected, or as required by law.

Your rights

You have the following rights with respect to your personal information:

- The right to access your personal information
- The right to correct any inaccuracies in your personal information
- The right to request that we delete your personal information
- The right to object to our processing of your personal information
- The right to restrict our processing of your personal information
- The right to data portability
- The right to complain to the Information Commissioner's Office (ico.org.uk)

These rights are in some circumstances, dependent on the legal basis your information is being processed.

How to contact us

If you have any questions about this privacy notice, please contact the School Data Privacy Lead at:

Knightsbridge School
67 Pont Street, London, SW1X 0BD
020 7590 9000

dataprotection@knightsbridgeschool.com

Changes to this privacy notice

We may update this privacy notice from time to time. The latest version will always be available on request.

KNIGHTSBRIDGE
SCHOOL

Appendix 3 - Data Breach Reporting Policy

This policy sets out the procedures for reporting data breaches at Knightsbridge School. It applies to all personal data processed by the school regardless of where it is stored or processed.

Examples of personal data breaches include:

- sending personal data to an incorrect recipient
- displaying personal data of pupils on a screen to other pupils
- the theft or loss of computing devices which contain personal data
- the alteration of personal data without permission
- unauthorised access to personal data on systems or paper

Responsibilities

The following individuals are responsible for reporting data breaches:

- The Data Protection Lead (DPL): is responsible for overseeing the school's data protection compliance and for investigating and reporting data breaches
- All staff: All staff are responsible for reporting any suspected data breaches to the DPO as soon as possible

Procedure

If you suspect a data breach has occurred, you should immediately report it to the DPL. The DPL will then investigate the matter and determine whether a data breach has actually occurred. If a data breach has occurred, the DPO will take the following steps:

1. Assess the impact of the breach
2. If necessary, notify the Information Commissioner's Office (ICO) within 72 hours of becoming aware of the breach
3. Notify the affected individuals if there is a high risk of their personal data being misused
4. Take steps to mitigate the impact of the breach
5. Review the school's data protection procedures to prevent future breaches

KNIGHTSBRIDGE
SCHOOL

Data Breach Notification

If a suspected data breach has occurred, the DPL will assess the incident and to determine the nature of the breach. If the breach poses a risk of abuse or harm to any data subject then the ICO will be notified within 72 hours of the school becoming aware of the breach. The notification will typically include the following information:

- The type of personal data that has been breached
- The number of individuals affected
- The likely consequences of the breach
- The measures that have been taken to mitigate the impact of the breach
- The contact details for the DPL

The school will also notify the affected individuals if there is a high risk of their personal data being misused. The notification will include the following information:

- The nature of the breach
- The personal data that has been affected
- The measures that have been taken to mitigate the impact of the breach
- Advice on how to protect themselves from further harm

Data Breach Response Plan

When	Action(s)
Immediately	● Notify the Data Protection Lead ● Start to record the particulars of the incident in a new Data Breach Report Form ● Depending on the level of the breach, the Data Protection Lead will involve relevant staff in the following stages. For the most serious breaches, a critical incident team will be formed. In all cases the Head & Group MD must be informed

Within the first few hours	• Determine the timescales of the breach, what data is involved and where that data has gone • Identify what immediate steps can be taken to contain the data now or to recover the data • If this is a cyber or electronic data breach, involve the school IT team • If people are involved, can they be contacted to give assurances • Determine if specialists are needed: e.g. IT security consultants, legal representatives
Within 72 hours	• Build a more complete picture of the breach – number of individuals affected, types of personal data involved (being particularly aware of any sensitive or financial data involved) and how the breach occurred • Identify if a crime has been committed and if so, involve the police • Assess the likely risk of harm to the individuals and decide whether the breach needs reporting to the ICO (and the individuals concerned) • Determine what can be done to mitigate the risk • Report to the ICO (and the individuals concerned), otherwise document rationale for not reporting • If technical, implement any fixes to ensure the same breach cannot easily reoccur
Within one week	• Continue to monitor and assess possible consequences • Review internally to identify how the breach occurred, how it could have been prevented, what follow-up action is needed to prevent a similar breach happening in the future • Where the ICO (and individuals) have been notified, keep them informed, as appropriate, as new information comes to light and tell them what is being done to improve practices
Within 1 month	• Data Protection Lead continues to keep a full internal record, whether or not the matter was reported to the ICO • Ensure any recommendations made by, or promised to, the ICO are actioned and make sure any follow-up action is implemented • Review policies and ensure regular (or specific) training is completed • Notify any other concerned parties (if required)
Ongoing	• Compare with past incidents to monitor and manage trends

KNIGHTSBRIDGE
SCHOOL

Data Breach Training

All staff will receive data breach training. The training will cover the following topics:

- The importance of data protection and cyber security
- Examples of common data breaches
- The procedures for reporting data breaches
- The procedures for escalating to the DPL and notifying the ICO and affected individuals
- Procedures for mitigating the impact of data breaches

How to contact us

If you have any questions about this data breach reporting policy, please contact the School Data Privacy Lead at:

Knightsbridge School
67 Pont Street, London, SW1X 0BD
020 7590 9000
dataprotection@knightsbridgeschool.com

Changes to this policy

We may update this privacy notice from time to time. The latest version will always be available on request.

KNIGHTSBRIDGE
SCHOOL

Appendix 3(i) - Template Data Breach Report Form for Staff

To be completed by the member of staff who first becomes aware of the breach and shared with the Data Privacy Lead , as soon as possible after the breach is identified. We have just 72 hours from the point that the first member of staff is aware of the breach in which to investigate the breach, assess the impact and notify the ICO if needed.

Please complete in as much detail as possible

Describe the data breach. What happened, the names of the people involved? When did the breach happen? Where did the breach happen? How and when did you become aware of the breach?
Whose data has been affected (lost, stolen, or shared or altered without proper authorisation)? What type of data is involved? Eg home address, email address, telephone number, assessment grades, medical details, SEN details. Was sensitive personal data involved? e.g. medical / SEN / financial?

If the data has been shared, who has it been shared with who should not have seen it?

Name of person reporting the personal data breach:	
Date & time of the report:	

KNIGHTSBRIDGE
SCHOOL

Appendix 3(ii) - Template Data Breach Report Form for Data Protection Lead

Information to be recorded in the breach register and, where necessary, given to the ICO when notifying them of the breach.

When and how did the School become aware of the breach?
Description of the data breach. What happened? When did the breach happen? Where did the breach happen? How did it happen?
How many people's data could be affected? Who could be impacted? (Category not names eg staff, pupils, parents/guardians). What sort of data has been breached?
What controls did you have in place that could have prevented the breach?

KNIGHTSBRIDGE
SCHOOL

What has been done to contain the breach or retrieve the data?
What risk is there to the individuals whose data this has impacted? What could be the impact? What is the likelihood that individuals will suffer serious consequences as a result of the breach?
Does this breach need reporting to the ICO (and individuals, where necessary)? Give reasons.
Actions that have been taken or will be taken to mitigate the impact for the individuals affected?
What has been learned? What actions need to be taken to avoid a similar breach happening in the future?

What other organisations or regulators have been or will need to be notified? When done, by whom?

Name of person reporting the breach to the ICO:	
Date & time of the report:	
Name of ICO contact:	
ICO Case #:	

KNIGHTSBRIDGE
SCHOOL

Appendix 4 - Data Subject Access Request Policy

This policy sets out the procedures for responding to data subject access requests (SARs) at Knights School. It applies to all personal data processed by the school regardless of where it is stored or processed.

Responsibilities

The following individuals are responsible for responding to DSARs:

- The Data Protection Lead (DPL): The DPL is responsible for overseeing the school's data protection compliance and for responding to DSARs.
- All staff: All staff are responsible for referring any DSARs to the DPL as soon as possible.

Procedure

If you receive a SAR, you should immediately refer it to the DPL. The DPL will then investigate the matter and determine whether the request is valid. If the request is valid, the DPL will take the following steps:

1. Verify the identity of the requester.
2. Assess the scope of the SAR, clarifying and refining this with the requester as required
3. Collate the personal information and redact others personal information as necessary to maintain their own confidentiality
4. Provide the requester with the information within one calendar month of receiving the request (or if the request is complex or the requester makes more than one, the response time may be a maximum of three calendar months, starting from the day of receipt)
5. Charge a reasonable fee for providing the information, if repeated or protracted SARs are made
6. Refuse to provide the information if there is an exemption or restriction that applies
7. Inform the requester of their right to complain to the Information Commissioner's Office (ICO)

KNIGHTSBRIDGE
SCHOOL

Making a SAR on Behalf of Someone Else

If the person requesting the information is a relative or representative of the individual concerned, then the relative or representative is entitled to personal data about themselves but must supply the individual's consent for the release of their personal data. If you have been appointed to act for someone, you must confirm your capacity to act on their behalf and explain how you are entitled to access their personal data. If you are the parent/guardian of a child over 13, we will need to consider whether the child can provide their consent to you acting on their behalf. Should you make a data subject access request but you are not the data subject, you must stipulate the basis under UK data protection legislation that you consider makes you entitled to the information.

Exemptions and restrictions

There are a number of exemptions and restrictions that may apply to DSARs. These include:

- The information is subject to legal privilege
- The information is confidential and would be likely to harm the requester or someone else
- The information is used for the prevention or detection of crime
- The information is used for the exercise of a public function

How to contact us

If you have any questions about this subject access request policy, please contact the School Data Privacy Lead at:

Knightsbridge School
67 Pont Street, London, SW1X 0BD
020 7590 9000
dataprotection@knightsbridgeschool.com

Complaints

If you are not satisfied with the way a SAR has been handled, you have the right to complain to the ICO.

Changes to this policy

We may update this privacy notice from time to time. The latest version will always be available on request.

KNIGHTSBRIDGE
SCHOOL

Appendix 5 - Data Retention Policy

The Data Retention Policy is one of a set of data protection policies to demonstrate compliance with current data protection legislation. Knightsbridge School aims to collect only the data that is necessary to run the school efficiently and effectively and to retain data for only as long as it is absolutely necessary.

The School's Data Protection Lead is responsible for the management of the School's data and in the event of any concerns about the handling of personal data they can be contacted at dataprotection@knightsbridgeschool.com.

Within the boundaries of the law and all statutory obligations placed on the School including safeguarding children in education, data will be retained according to the schedule below:

General School Records

Type of Record/Document	**Retention Period**
School registration documents	Permanent (or until closure of the school)
Pupil attendance register	3 years from the date of last entry
Minutes of Governors / Directors meetings	Permanent
Annual curriculum	3 years from the end of academic year
Class data - e.g timetables, marks, assignments	1 year from the end of academic year

Individual Pupil Records

Type of Record/Document	**Retention Period**

Pupil admissions: application forms, assessments, records of decisions	25 years from date of birth. If pupil not admitted, up to 7 years from that decision or for as long as a pupil could be offered a place at the school
Pupil examination Results (internal & external)	7 years from the pupil leaving the school
Pupil file (including pupil reports, performance records, medical records)	25 years from date of birth (except where relevant safeguarding considerations apply - any material that may be relevant should be kept for the lifetime of a pupil)
Pupil special educational needs records	35 years from date of birth (allowing for extensions to statutory limitation period)

Safeguarding Children

Type of Record/Document	**Retention Period**
Policies & procedures	Permanent
DBS certificates / checks	DBS certificates never held. Check records are held permanently
Accident / incident reports	Keep on record for as long as any living victim may bring a claim (Note - all civil claim limitation periods are set aside in cases of abuse). Ideally, files to be reviewed from time to time if resources allow and a suitably qualified person to make the judgement is available
Child protection files	Indefinitely to comply with IICSA

Corporate Records

Type of Record/Document	**Retention Period**

Certificate of incorporation	Permanent or until dissolution of the company
Minutes, notes and resolutions of Board and Management meetings	Permanent or until dissolution of the company
Shareholder resolutions	Permanent or until dissolution of the company
Register of members and shareholders	Permanent or until dissolution of the company (10 years for ex-members or ex-shareholders)
Annual reports	6 years minimum

Accounting Records

Type of Record/Document	**Retention Period**
Financial Accounting Records	6 years minimum
Tax Returns	6 years minimum
VAT Returns	6 years minimum
Internal financial reports and budgets	3 years minimum

Employee & Employment Records

Type of Record/Document	**Retention Period**
Single Central Record of employees	Keep a permanent record of checks that have been made

Contracts of employment	7 years from the effective end date of the contract
Staff appraisals & reviews	7 years from the end of employment
Staff personnel files	25 years from the end of employment but retain any material that may be relevant to a safeguarding claim
Payroll, salary, maternity & sick pay records	7 years minimum
Pension & benefits schedule records	Permanent
Job application, interview notes & rejection letters for unsuccessful candidates	Date of interview notes + 6 months. If successful place in personnel file
Staff training records	7 years from the end of employment
Immigration records	7 years minimum
Employee health records	7 years from the end of employment
Directors & governors	Permanent
Alumni	Lifetime unless they inform the school otherwise

Insurance Records

Type of Record/Document	**Retention Period**
Insurance policies (various)	Duration of policy (or as required by policy) plus a period for any run-off arrangement and coverage of insured risks)
Correspondence related to claims, renewals or notifications	7 years minimum

Liability policies (public, employers etc)	Permanent

Environment & Health Data

Type of Record/Document	**Retention Period**
Service / maintenance logs	Permanent
Child accident reports	25 years from date of birth or longer where safeguarding is concerned
Adult accident at work reports	7 years from date of accident minimum
Staff use of hazardous substances	7 years from end of date used minimum
Risk assessments	3 years from the completion of a project, incident, event or activity
Data protection records	For as long as they are current and relevant. For data breach records that contain personal data 7 years from the date of the incident or event

Contracts & Agreements

Type of Record/Document	**Retention Period**
Deeds or contracts under seal	Minimum – 13 years from completion of contractual obligation or term of agreement
Contracts with customers, suppliers, agents or others	6 years after contract expiry or completion

Rental and hire purchase agreements	6 years from the end of the agreement
Licensing and subscription agreements	6 years from the end of the agreement

Intellectual Property Records

Type of Record/Document	**Retention Period**
Formal documents of title (trade mark or registered design certificates; patent or utility model certificates)	Permanent in the case of any right which can be permanently extended, eg trade marks; otherwise expiry of right plus 7 years minimum
Assignments of intellectual property to or from the school	Expiry of right plus 7 years minimum or with deeds, 13 years
IP / IT agreements (including software licences and ancillary agreements e.g. maintenance; storage; development; coexistence agreements; consents)	7 years from completion of contract or the term of agreement

KNIGHTSBRIDGE
SCHOOL

Appendix 6 - Technical and Organisational Security Measures

Knightsbridge School will use appropriate technical and organisational measures to keep personal information secure, to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage.

All staff are responsible for keeping information secure in accordance with the legislation and must follow the school's acceptable usage policy at all times.

The school has developed and will maintain safeguards appropriate to its size, scope and business, its available resources, the amount and categories of personal data that it holds. It will periodically evaluate and test the effectiveness of those safeguards to ensure security of processing.

Staff must guard against unlawful or unauthorised processing of personal data and against the accidental loss of, or damage to personal data. Staff must exercise particular care in protecting sensitive personal data from loss and unauthorised access, use or disclosure.

Staff must follow all procedures and technologies put in place to maintain the security of all personal data from the point of collection to the point of destruction. Staff may only transfer personal data to third-party service providers who have been assessed as meeting the same or better standards of data security and privacy as those required by the school and UK data protection legislation.

Staff must maintain data security by protecting the **confidentiality, integrity and availability** of the personal data, defined as follows:

Confidentiality means that only people who have a need to know and are authorised to use the personal data can access it.

Integrity means that personal data is accurate and suitable for the purpose for which it is processed.

Availability means that authorised users can access the personal data when they need it for authorised purposes.

Staff must comply with and not attempt to circumvent the administrative, physical and technical safeguards the school has implemented and maintains to protect personal data.

Where the school uses external organisations to process personal information on its behalf, contracts with external organisations must provide that:

- the organisations are subject to and uphold UK data protection legislation or work under a jurisdiction that has met UK GDPR adequacy regulations or appropriate safeguards such as the EU-US Data Privacy Framework
- those processing data are subject to the duty of confidence
- appropriate technical and operational measures are taken to ensure the integrity, availability and security of data processing
- the organisation will provide suitable mechanisms for the school to conduct subject access requests on behalf of data subjects
- the organisation will delete or return all personal information to the school as requested at the end of the contract
- the organisation will provide the means to audit the data held on behalf of the school

- tell the school immediately if it does something infringing data protection law

Before any new agreement involving the processing of personal information by an external organisation is entered into, or an existing agreement is altered, the relevant staff must always gain approval from the school DPL.