KNIGHTSBRIDGE
SCHOOL

Knightsbridge School Data Protection Policy

As part of its normal operation Knightsbridge School collects, stores and processes a wide range of data especially information concerning 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. 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, a breach of this policy could 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 seven principles of the 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, 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.

KNIGHTSBRIDGE
SCHOOL

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, 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 or cloud accounts or services 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 should 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.

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 signing up to or adopting a web based service or account at school - does the provider comply with GDPR? Do they act as a data processor or assume data controller rights? Have I followed the approval process for signing up and using the account for school purposes?
- How can I ensure the personal data I need to work with does not reside on my personal device or computer? If unsure, always ask the Data Protection Lead

Data protection law is a code of useful and sensible checks and balances to 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.

KNIGHTSBRIDGE
SCHOOL

Appendix 1 - Data Privacy Notice(s)s

Template Knightsbridge School Data Privacy Notice - Prospective Parents and Pupils

Before formally joining Knightsbridge School, we will be in contact with a wide variety of parents, pupils and guardians and this privacy notice explains how we manage this
personal data.
When parents sign the acceptance form and their child begins at School, they become
subject to the Parent Terms and Conditions and these include a full privacy notice detailing
how the School manages their data and the legal basis used for that processing.

What data do we collect?

The personal data that the Registrar will collect may consist of:

For the candidate:

- Name
- date of birth
- address details
- Feeder and previous schools' information
- Information on siblings (if given)
- school report(s) and confidential reference(s)
- Reports from extracurricular activities and/or tutors (if relevant)
- Educational Psychologist report (if relevant and shared with the school)
- Medical Reports (if relevant)
- Special health/food/allergies requirements (if relevant)
- bursary application details (we do not hold the financial information)
- Test results (internal and external)
- Interview comments/results
- Passport information (and visa information if requires visa)
- Guardian/agent details (name, address, email and telephone number)

For the parents:

KNIGHTSBRIDGE
SCHOOL

- Name
- Address, email, telephone numbers
- Occupation
- Marital status
- Details, if required, of parental responsibility that you may have given us when originally

enquiring about the School, at the time of registration, or subsequently;

Data about prospective parents and children will usually be collected directly from you but some data may be collected from third parties (for example previous schools, confidential references).

How we use your data

The legal basis for holding your data is 'legitimate interest'. The School needs your personal data in order to successfully manage and administer the admissions process. Sensitive personal data is sometimes collected and generally held in order to protect you or your child's vital interests, safeguard your child or as a result of legal obligation.
We will also ask for specific consent at the time of registration or initial expression of interest to send you future information about the School (prospectuses, upcoming events such as open days, newsletters etc). You will have the option to choose not to receive these further marketing communications at any time after your initial enquiry and to withdraw this consent if previously given.
Your personal data will be processed strictly in accordance with the DPA and GDPR and in the legitimate interests of the School in order to:

- Communicate and promote the School's admissions events and activities (that you have

consented to)

KNIGHTSBRIDGE
SCHOOL

● Advise you about the next steps in the application process (ie Taster days, Assessment
date and details, Interviews, Results, Induction days)
● Make decisions concerning admissions

Who has access to your data

Data about prospective parents and children is held securely in a database and paper files
belonging to Knightsbridge School and is treated confidentially and with sensitivity. Such data may be made available upon request to academic and administrative departments involved in the admissions process at the Schools. The data will not be disclosed to third parties (except where required by legal or other statutory obligation) or
external organisations and the data is not transferred overseas (other than results sent back
to those in their countries of origin).

How long do we keep your data?

Personal data is kept for the purposes of the administration of admissions
and is kept for the length of time a pupil would have been able to attend the School.

Subject rights under the DPA/GDPR

All data subjects have certain rights under the General Data Protection Regulation and the
UK Data Protection Bill, including a right to be given access to data held about them by any
data controller and a right to be removed from our database should you no longer wish to
receive information from the School.
You also have the right to opt out of the use of your data for any of purposes specified above provided it is not required to administer the admissions process in which you wish to participate. Should you wish to opt out or be removed from our database or access your data, please contact registrar@knightsbridgeschool.com

If you have any concerns about the School's handling of your personal data, please contact
James Prior, (Data Protection Officer) (dataprotection@knightsbridgeschool.com).

How to complain

You can also complain to the ICO if you are unhappy with how we have used your data. The ICO's address is:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF
Helpline Number: 03031 231113

Template Knightsbridge School Data Privacy Notice - Parents and Pupils

School contact details

Name: Knightsbridge School

Address: 67 Pont Street, London, SW1X 0BD

Phone Number: 020 7590 9000

E-mail: dataprotection@knightsbridgeschool.com

What type of information we have

We currently collect and process the following information:

- Personal identifiers, contacts and characteristics (for example, name and contact details, address and unique pupil number)
- Characteristics (such as ethnicity and language)
- Safeguarding information (such as court orders and professional involvement)
- Special educational needs (including the needs and ranking)
- medical and administration (such as doctors information, child health, dental health, allergies, medication and dietary requirements)

- Attendance (such as sessions attended, number of absences, absence reasons and any previous schools attended)
- Assessment and attainment (such as key stage 1 and phonics results and any relevant results)
- Behavioural information (such as exclusions and any relevant alternative provision put in place)
- School trips and after school activities

How we get the information and why we have it

Most of the personal information we process is provided to us directly by you when you complete our registration form, from former educational settings or simply in the ordinary course of interaction or communication (such as email or written assessments). . We have this information for the following reasons:

- To support pupil learning
- To monitor and report on pupil attainment progress
- To provide appropriate pastoral care
- To assess the quality of our services
- To keep children safe (dietary requirements, food allergies, or emergency contact details)
- To meet the statutory duties placed upon us for DfE data collections
- Payment of fees and other charges
- Maintain the school community (e.g. newsletters, Parent's Association, Alumni.)

We routinely share pupil information with:

- Schools that the pupils attend after leaving us
- The Department for Education (DfE)
- The Local Authority
- appropriate regulatory bodies e.g. the Independent Schools Inspectorate.
- NHS

Under the General Data Protection Regulation (GDPR), the lawful bases we rely on for processing this information are:

(a) Your consent. You are able to remove your consent at any time. You can do this by contacting The Data Protection Officer, email dataprivacy@knightsbridgeschool.com, telephone 020 7590 9000.

(b) We have a contractual obligation.

(c) We have a legal obligation.

(d) We have a vital interest.

(e) We need it to perform a public task.

(f) We have a legitimate interest.

How we store your information

Your information is securely stored in the following methods depending on the nature of the material:

- In a filing cabinet within a locked room with access only by authorised personnel.
- Digitally on our secure local file servers and secure cloud based servers. Accessed only by authorised personnel.

Please refer to our Data Retention Schedule to see how long we retain each category of data held.

We will then dispose your information by

- Secure shredding by an authorised secure data destruction company
- Physical digital storage (e.g. hard drives) destroyed by a WEEE certified destruction company

- Electronic digital information permanently deleted

Your data protection rights

Under data protection law, you have rights including -

- **Right of access** - You have the right to ask us for copies of your personal information
- **Right to rectification** - You have the right to ask us to rectify information you think is inaccurate. You also have the right to ask us to complete information you think is incomplete
- **Right to erasure** - You have the right to ask us to erase your personal information in certain circumstances
- **Right to restriction of processing** - You have the right to ask us to restrict the processing of your information in certain circumstances
- **Right to object to processing** - You have the right to object to the processing of your personal data in certain circumstances
- **Right to data portability** - You have the right to ask that we transfer the information you gave us to another organisation, or to you, in certain circumstances

You are not required to pay any charge for exercising your rights. If you make a request, we have one month to respond to you.

Please contact us using the details at the top of this notice if you wish to exercise any of your rights as a data subject under law or if you wish to make a data access request.

How to complain

You can also complain to the ICO if you are unhappy with how we have used your data. The ICO's address is:

Information Commissioner's Office
Wycliffe House
Water Lane

KNIGHTSBRIDGE
SCHOOL

Wilmslow
Cheshire
SK9 5AF
Helpline Number: 03031 231113

KNIGHTSBRIDGE
SCHOOL

Template Knightsbridge School Data Privacy Notice - Staff

Employee Privacy Notice

Who does this apply to?

This privacy notice applies to employees and workers of Knightsbridge School and those applying
to work at Knightsbridge School. It also applies to former employees and workers at Knightsbridge
School and contractors.

Why do we collect and use employee information? (Lawful basis for processing)

We collect and use employee information under section 6(1)(b) of the GDPR which states
'Processing is necessary for the performance of a contract with the data subject or to take steps to
enter into a contract' and article 9(2)(b) 'The processing is necessary in the context of employment
law, or laws relating to social security and social protection.'

Therefore, we collect and process your data:

- for the school's legitimate interests
- to ensure that we can meet the terms of your contract of employment
- for your health, safety and welfare
- for child protection and other regulatory purposes

We use employee data to:

- carry out required legal background checks (DBS)
- ensure employees have a right to work in the UK
- ensure employees receive their salary and pension contributions
- monitor and review performance and pay
- monitor sickness and absence levels
- fulfil our duty of care to employees
- enable a comprehensive picture of our staffing and how it is deployed

KNIGHTSBRIDGE SCHOOL

• inform the development of recruitment and retention policies
• support our financial modelling and planning

The categories of employee information that we collect, hold and share include:

• Personal information (such as name and address)
• Financial information (such as bank account data, National Insurance number, tax code)
• Characteristics (such as language, nationality, country of birth)
• Sickness and absence information
• Relevant medical information

Collecting employee information

Whilst the majority of information you provide to us is mandatory, some of it is provided to us on a
voluntary basis. In order to comply with the General Data Protection Regulation, we will inform you
whether you are required to provide certain information to us or if you have a choice in this. There is no automated decision making or profiling which is undertaken with your data.

Storing data

We store our employee data in locked files and on a secure area of our server which can be accessed only by the HR team. Line Managers are entitled to access the performance management information of their team members.

We retain information as follows:

Single Central Register	Indefinite
Contract of Employment	Duration of employment plus 25 years
Appraisals and performance management documents*	Duration of employment plus 25 years
Personnel file*	Duration of employment plus 25 years
Payroll and salary records	7 years

Pension records	Indefinite
Job Application and interview records	Up to 1 year from date of application
Immigration Records	Duration of employment plus 4 years
Health Records*	Duration of employment plus 7 years

* Information may be retained for a longer duration if child protection matters require this.

We routinely share employee information with:

- Pensions authorities – TPS, People's Pension
- DBS Clearance provider – Atlantic Data
- Payroll company – Payroll management
- The Department for Education (DfE)
- Directors and Advisors of the Knightsbridge School Ltd
- Auditors
- Consultants engaged to advise on HR and Staff Development
- IT Contractor

It is not necessary for data to be transferred abroad. The exception to this will be international trips
that the school organises; should this be envisaged for you, you will be contacted for your consent,
the consent will be limited in time and content if it be required.

Requesting access to your personal data

Under data protection legislation, employees have the right to request access to information about

them that we hold. To make a request for your personal information contact the Data Protection Officer.

We respectfully request that although you are under no legal obligation to do so, you request
information during term time to give the school the best opportunity to comply with your request
within one month.

You also have the right to:

• object to processing of personal data that is likely to cause, or is causing, damage or distress

• prevent processing for the purpose of direct marketing

• object to decisions being taken by automated means

• in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and

• claim compensation for damages caused by a breach of the Data Protection regulations

If you have a concern about the way we are collecting or using your personal data, you should
raise your concern with us in the first instance, (James Prior, Data Protection Officer) or directly to the Information Commissioner's Office
at https://ico.org.uk/concerns/

Contact:

If you would like to discuss anything in this privacy notice, please contact James Prior (Data Protection Officer) j.prior@knightsbridgeschool.com

KNIGHTSBRIDGE
SCHOOL

Appendix 2 - Special Category Data Policy

This policy sets out:

- how we will comply with the data protection principles to process special category personal data
- how we will handle special category data that we process, our lawful basis and purpose of processing and the relevant condition for processing under GDPR and data protection law

This policy document will be retained, reviewed and (if appropriate) updated by the Data Protection Officer and (if requested) made available to the Information Commissioner, until six months after we cease carrying out the processing.

1. Special category data at a glance

Special category data is personal data which the General Data Protection Regulations (GDPR) says is more sensitive, and so needs more protection. In order to lawfully process special category data, we must identify both a lawful basis under GDPR and a separate condition for processing special category data.

The special categories are personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of 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.

The special category personal data that we may process are ethnic origin, biometrics (where used for ID purposes for door entry), health and school specific sensitive data which may include but not limited to SEN/AEN. and child protection.

The provision of equality monitoring data such as race or ethnic origin and heath (disability) is optional in some circumstances.

2. Principles

KNIGHTSBRIDGE
SCHOOL

The General Data Protection Regulations (GDPR) has 6 principles that we must follow when collecting and using personal information and to comply we must take steps to make sure all personal information is:

- processed lawfully, fairly and in a transparent manner
- collected for specified, explicit and legitimate purposes
- adequate, relevant and limited to what is necessary
- accurate and up to date
- kept in a form which permits identification of data subjects for no longer than is necessary processed securely

The special conditions under GDPR which allow processing of special category personal data are:

- Article 9(2) (a) – explicit consent has been given.
- Article 9(2) (b) – for employment, social security and social protection purposes. · Article 9(2) (c) – for vital interests.
- Article 9(2) (d) – for legitimate activities by a foundation, association or any other not for profit body with political, philosophical or religious or trade union aim.
- Article 9(2) (e) – for employment, social security and social protection purposes. · Article 9(2) (f) – for defence of legal claims.
- Article 9(2) (g) – for substantial public interest purposes.
- Article 9(2) (h) – for health and social care purposes.
- Article 9(2) (i) – for public health purposes.
- Article 9(2) (j) – for archiving, research and statistics purposes.

Conditions relating to the processing of the special categories of personal data

Schedule 1 of the Data Protection Act 2018 establishes conditions that permit the

processing of the special categories of personal data and criminal convictions data. The Schedule is split into four parts:

- Part 1 – Conditions relating to employment, health and research
- Part 2 – Substantial public interest conditions
- Part 3 – Additional conditions relating to criminal convictions
- Part 4 – Appropriate policy document and additional safeguards

Schedule 1 of the Data Protection Act 2018 establishes conditions that permit the processing of the special categories of personal data as follows:

- The processing of the special categories of personal data meets the requirements in points (b), (h), (i) or (j) of Article 9(2) of the GDPR if it meets one of the conditions listed in Part 1 of Schedule 1.
- The processing of the special categories of personal data meets the requirement in point (g) of Article 9(2) of the GDPR if it meets one of the conditions listed in Part 2 of Schedule 1.

3. Schedule 1 Conditions that are relevant to Knightsbridge School

a) Schedule 1, Part 1 conditions for processing in connection with employment, health and research that are relevant to us are:

- Employment, social security and social protection: Processing necessary for the purposes of performing or exercising obligations or rights of the controller or the data subject under employment law, social security law or the law relating to social protection.
- Health or social care: Processing necessary for health or social care purposes.

b) Schedule 1, Part 2 conditions for processing in the substantial public interest that are relevant to us are:

- Statutory and government purposes: Processing necessary for the exercise of a function conferred on a person by enactment or the exercise of a function of the Crown, a Minister or a government department.
- Equality of opportunity or treatment: Processing necessary for identifying or keeping under review the existence or absence of equality of opportunity or treatment between groups of people with the view to enabling such equality to be promoted or maintained.
- Counselling etc

- Safeguarding of children and individuals at risk

4. The processing of special category personal data by us

a) Ethnic origin (Students)

- Purpose: Required by the DfE for Census purposes.
- GDPR Article 6 (1) (e) Public task, Article 9 (2) (g) substantial public interest.
- Data Protection Bill Schedule 1 part 2, 1 condition: statutory and government purpose.

b) Ethnic origin (Staff)

- Purpose: Equality and diversity.
- Law: Equality Act 2010 and associated regulations.
- GDPR Article 6 (1) (e) Public task, Article 9 (2) (g) substantial public interest.
- Data Protection Bill Schedule 1 part 2, 3 condition: equality of opportunity or treatment.

c) Student Counselling

- Purpose: Advice and support for students
- Law: Children and Young Peoples Act 1989
- GDPR Article 6 (1) (e) Public task, Article 9 (2) (g) substantial public interest.
- Data Protection Bill Schedule 1 part 2, 17 condition Counselling etc.

d) Safeguarding of children

- Purpose: Advice and support for students
- Law: Children and Young Peoples Act 1989
- GDPR Article 6 (1) (e) Public task, Article 9 (2) (g) substantial public interest.
- Data Protection Bill Schedule 1 part 2, 18 condition Counselling etc.

5. The purposes of the processing

To deliver a balanced and broadly based curriculum which - promotes the spiritual, moral, cultural, mental and physical development of pupils at the school and within society, and prepares pupils for the opportunities, responsibilities and experiences of later life. This includes school trips and activities; where appropriate counselling

services and child safeguarding.

Appendix 3 - Data Breach Reporting Policy

Knightsbridge School is committed to personal data protection and has policies, systems, security and appropriate staff training in place to achieve this. Despite this there is always a risk that a data breach may occur and this policy sets out the process and procedures for dealing with these incidents.

Under the current UK data protection legislation all data breaches that occur within the school must be recorded and this will be done so on the school Data Breach Register. The breaches that are assessed as likely to result in "a risk to the rights and freedoms of natural persons" will be reported to the Information Commissioner's Office (ICO) within 72 hours of the School being aware of the breach. Where the breach is deemed likely to result in "a high risk to the rights and freedoms of natural persons" the individuals affected will be notified without undue delay.

What is meant by a personal data breach?

A personal data breach is a security incident that has affected the confidentiality, integrity or availability of personal data. Data breaches can be a result of both accidental and deliberate causes. It is classed as a personal data breach whenever any personal data is:

- lost
- destroyed (except planned deletions in line with the School's retention policy)
- corrupted
- disclosed (if someone accesses the data who should not have or passes it on without proper authorisation), or
- made unavailable (and this unavailability has a significant negative effect on individuals)
- 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

KNIGHTSBRIDGE
SCHOOL

How to report a data breach

All data breaches that occur within the School need to be reported to the Data Protection Lead at dataprotection@knightsbridgeschool.com Any data breaches that occur at one of the School's third party data processors that impact personal data from the School also need to be reported to the Data Protection Lead. All data breaches must be investigated and documented in the School's internal Data Breach Register by the Data Protection Lead, in accordance with the procedure laid out in this policy.

If a data breach is considered *likely* to result in discrimination, damage to reputation, identity theft or fraud, financial loss, loss of confidentiality or any other significant economic or social disadvantage then it will be reported to the ICO within 72 hours of the School being aware of the breach. Breaches can be reported to the ICO using their personal data breach helpline, 0303 123 1113. Breaches will be reported to the ICO by the Data Protection Lead.

When reporting a breach to the ICO, the following information will be provided:

- a description of the nature of the personal data breach including:
    - the categories and approximate number of individuals concerned
    - the categories and approximate number of personal records concerned
- the name and contact details of the Data Protection Lead
- a description of the likely consequences of the personal data breach, and
- a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

If it is not possible to investigate the breach fully within 72 hours, it is acceptable to provide this information to the ICO in phases but the initial notification must be within the first 72 hours.

If a data breach is considered *highly likely* to result in discrimination, damage to reputation, identity theft or fraud, financial loss, loss of confidentiality or any other significant economic or social disadvantage then it will be reported to the ICO within 72 hours of the School being aware of the breach *and to the individual(s) whose data was involved without undue delay*. The ICO will give guidance as to whether a data breach has reached this higher category and requires individuals to be notified.

In notifying individuals of a data breach the following information must be given:

- a description of the nature of the personal data breach
- the name and contact details of the Data Protection Lead
- a description of the likely consequences of the personal data breach, and

- a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures the School has taken to mitigate any possible adverse effects and any action the individual(s) can take themselves to mitigate these effects

Where it is considered that a breach does meet either criteria above and the ICO (and individuals) are not notified the rationale for the decision will be documented and included in the breach register.

Whenever a data breach is reported to the ICO, the School may also need to inform other organisations or concerned third parties including where deemed necessary, the police.

The procedure to follow on discovering a breach

The following table describes the process that the school will follow when investigating a breach, taking appropriate actions to mitigate the breach and where necessary, notifying the ICO and any individuals concerned. All the actions and information relevant to each stage need to be documented and recorded in the School Breach Register, regardless of whether a breach is notified to the ICO or not.

KNIGHTSBRIDGE SCHOOL

When	Action(s)
Immediately	• Notify the Data Protection Lead • Start to record the particulars of the incident in a new Data Breach Report Form (see below) • 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 & Principal 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

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

KNIGHTSBRIDGE
SCHOOL

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?

KNIGHTSBRIDGE
SCHOOL

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?

KNIGHTSBRIDGE
SCHOOL

What controls did you have in place that could have prevented the breach?
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.

KNIGHTSBRIDGE
SCHOOL

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 document sets out the schools policy for responding to subject access requests under current UK data protection legislation.

Current UK data protection legislation gives individuals ("data subjects") the right to know what information is held about them. It provides a framework to ensure that personal data is handled properly. It requires organisations who collect, hold, use, amend, share and delete ("process") personal data to do so fairly and reasonably and only for the purpose they have stated. It provides individuals with important rights, including the right to know what personal data is held electronically and on paper and for their "right to be forgotten" in some circumstances.

The school is committed to operating openly and transparently and meeting all reasonable individual requests for personal data ("subject access requests") that are not subject to specific exemption.

How to make a subject access request?

A subject access request is a written request (in writing to the Head / Data Protection Lead or by email to dataprotection@knightsbridgeschool.com) for personal data held about you, or if a parent guardian, about your child by the school. Generally, data subjects have the right to see what personal data we hold about them. However, this right is subject to certain exemptions that are set out in law.

What is personal data / information?

Information which is biographical or which has the individual as its focus.

What do we do when a subject access request is received?

We will first check that we have enough information to be sure of your identity. Often we will have no reason to doubt a person's identity; for example, if we have regular contact with them. However, if we are unable to identify you we will ask you to provide evidence we reasonably need to confirm your identity. For example,

we may ask you for a piece of information held in your records that we would expect you to know, a proof of name and address, identity or similar.

If the person requesting the information is a relative/representative of the individual concerned, then the relative/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 the GDPR that you consider makes you entitled to the information.

Collation of information

- We will check that we have enough information to find the records you requested. If we feel we need more information, then we will promptly ask you for this.
- We will gather any paper or electronically held information and identify any information provided by a third party or which identifies a third party.
- We do not have the right to share any information about any third party with you unless the other party has provided their explicit consent or it is determined to be reasonable to do so without their consent.
- Before sharing any information that relates to third parties, we will, where possible, anonymise information that identifies third parties not already known to the individual (e.g. the school's employees) and edit information that might affect another party's privacy. We may also summarise information rather than provide a copy of the whole document.

Issuing our response

- Once any queries around the information requested have been resolved, you will be provided with a copy of the information except where it is impossible or where it would involve undue effort. In such cases, you will be offered the opportunity to view the information at the School, which may be on a screen

- We will explain any complex terms or abbreviations contained within the information as necessary.

Will we charge a fee?

All data subjects have the right of access to the data the school holds about them free of charge. However repeated or protracted subject data requests may incur a reasonable charge under the terms of the current legislation.

What is the timeframe for responding to subject access requests?

Information will be provided without delay and at the latest within one month of receipt of the request.
We may extend the period of compliance by a further two months where requests are complex. If this is the case, we will inform the individual within one month of the receipt of the request and explain why the extension is necessary.

Are there any grounds we can rely on for not complying with a subject access request?
If you have made a previous subject access request we must respond if a reasonable interval has elapsed since the previous request. A reasonable interval will be determined based on the nature of the information, the time that has elapsed, and the number of changes that have occurred to the information since the last request.

What is exempt from subject access requests?

Current data protection legislation contains a number of exemptions to our duty to disclose personal data and we may seek legal advice if we consider that they might apply. Possible exemptions include -

- information covered by legal or professional privilege
- confidential references given or received by the school
- Examination answers written by candidates (but not the information recorded by the marker)
- Negotiations where the data protection provisions could prejudice any negotiation with the individual

KNIGHTSBRIDGE
SCHOOL

What if you identify an error in our records?

If we agree that the information is inaccurate, we will correct it. We will consider whether any relevant third party needs to be advised of the correction. If we do not agree or feel unable to decide whether the information is inaccurate, we will make a note of the alleged error and keep this on file.

What if you want the School to stop processing your data?

You can object to the School processing your data altogether or request the School to delete your personal data. However, this only applies to certain processing activities (refer to the relevant Privacy Notice).

What if I'm not satisfied with the school's response to my data request?

If you are not satisfied by our actions, please contact the school's Data Protection Lead by email dataprotection@knightsbridgeschool.com or via the school reception office. If you are unable to reach a satisfactory outcome, you can seek recourse through the school's official complaints procedure. If you are still not satisfied, you can contact the Information Commissioner on 0303 123 1113 (https://ico.org.uk)

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

KNIGHTSBRIDGE
SCHOOL

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, 67 Pont Street London SW1X 0BD t: 020 7590 9000 f: 020 7589 9055
e:info@knightsbridgeschool.com www.knightsbridgeschool.com
Knightsbridge School Limited Registered Office: 11t Floor, 76 Shoe Lane London EC4A 3JB. Registered England no. 5759164

KNIGHTSBRIDGE
SCHOOL

Appendix 6 - Technical and Organisational Security Measures

Information Security

The 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 their school's acceptable usage policy.

The school will develop, implement and maintain safeguards appropriate to its size, scope and business, its available resources, the amount of personal data that it owns or maintains on behalf of others and identified risks (including use of encryption and pseudonymisation where applicable). It will regularly 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 agree in writing to comply with the required policies and procedures and who agree to put adequate measures in place, as requested.

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.

KNIGHTSBRIDGE
SCHOOL

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 in accordance with the GDPR and DPA.

Where the school uses external organisations to process personal information on its behalf, additional security arrangements need to be implemented in contracts with those organisations to safeguard the security of personal information. Contracts with external organisations must provide that:

- the organisation may only act on the written instructions of the school
- those processing data are subject to the duty of confidence
- appropriate measures are taken to ensure the security of processing
- sub-contractors are only engaged with the prior consent of the school and under a written contract
- the organisation will assist the school in providing subject access and allowing individuals to exercise their rights in relation to data protection
- the organisation will delete or return all personal information to the school as requested at the end of the contract
- the organisation will submit to audits and inspections, provide the school with whatever information it needs to ensure that they are both meeting their data protection obligations, and tell the school immediately if it does something infringing data protection law

KNIGHTSBRIDGE
SCHOOL

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 seek approval from the DPO.

KNIGHTSBRIDGE
SCHOOL

Appendix 7 - Data protection documentation

For compliance with current data protection legislation in the UK the school documents the following information:

- The name and contact details of our organisation, Data Protection Lead (and where applicable, any other controllers)
- The purposes of the personal data processing activities undertaken
- A description of the categories of individuals and categories of personal data
- The categories of recipients of personal data
- Details of any transfers to third countries including documenting the transfer mechanism safeguards in place
- Retention schedules
- A description of our technical and organisational security measures

In assisting with our data protection obligations the school may also choose to document the following -

- information required for privacy notices, such as:
    - the lawful basis for the processing
    - the legitimate interests for the processing
    - individuals' rights
    - the existence of automated decision-making, including profiling
    - the source of the personal data;
- records of consent;
- controller-processor contracts;
- the location of personal data;
- Data Protection Impact Assessment reports;
- records of personal data breaches;
- information required for processing special category data or criminal conviction and offence data under the Data Protection Act 2018, covering:
    - the condition for processing in the Data Protection Act;

- the lawful basis for the processing in the UK GDPR; and
- Data retention policy document.

KNIGHTSBRIDGE
SCHOOL

Appendix 8 - Useful Definitions

- **Privacy notice** - a statement made to data subjects that describes how the organization collects, uses, retains and discloses personal information
- **Lawful grounds for data processing** or **the legal basis of processing** - one of six lawful reasons for processing personal data as defined in GDPR, May 2018
- **Data subject rights** - the rights that individuals have under data protection law
- **Data subject access request** - the right of a data subject to request access to their personal data held by an organisation. This must be free of charge (at least in the first instance) and the personal data made available within 28 days of the data subject access request
- **Data controller** – an organisation that determines the purpose and means of the processing of personal data. For example, the school is the controller of pupils' personal data. As a data controller, we are responsible for the safeguarding of this data.
- **Data processor** – an organisation that processes personal data on behalf of a data controller. Examples at school include email, classroom management, payroll, finance, web filtering, providers, amongst others.
- **Data Subject** - a living individual who can be identified by the personal data
- **Personal data breach** – a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.
- **Personal data** or **personal information** - any information relating to a living individual (a data subject), including name, identification number, location or online identifier such as an email address. Note that personal information created in the ordinary course of work duties (such as in emails, notes of calls, and minutes of meetings) is still personal data and regulated by data protection laws, including the GDPR. Note also that it includes expressions of opinion about the individual or any indication of someone's intentions towards that individual.
- **Processing** – virtually any activity done with personal data, 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 in print); altering it or deleting it.
- **Special categories of personal data** – data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health and medical conditions, sex life or sexual orientation, genetic or biometric data used to identify an individual. Special categories of personal data also include employment

records and safeguarding records . There are also separate rules for the processing of personal data relating to criminal convictions and offences.