Data Protection Policy

Version 1.0 – March 2018

Owner: Ms Sophie Allen - Headteacher

Review Date: March 2019

Version control table

Version Number	Date	Purpose/Change	Reviewer / Authoriser
1.0	01/03/2018	Policy created	Data Protection Officer on behalf of The Stonebridge School

Contents

1 About this document 4
2 Scope 4
3 Policy statement 5
4 Responsibilities 6
5 The Data Protection Principles 10
6 Data subject(s)' rights 14
7 Consent 15
8 Security of data 15
9 Disclosure of data 16
10 Retention and disposal of data 16
11 Data transfers 17
12 Record of Processing Activities (RoPA) 17
13 Data breaches 18
14 Concerns about data protection 18
15 Further information 18
Appendix 1 – Glossary of Terms 20

1 About this document

This document incorporates the EU General Data Protection Regulation (GDPR) and the UK Data Protection Act 2018 that together supersedes the Data Protection Act 1998. The purpose of this document is to state the Stonebridge School's policy in protecting the "rights and freedoms" of natural persons (i.e. living individuals), to ensure that personal data is not processed without their knowledge, and wherever possible that it is processed with their consent.

2 Scope

This Policy applies to **all personal data** processed by The Stonebridge School in carrying out its operational activities.

This policy applies to all of The Stonebridge School' s personal data processing functions, including those performed on pupils', clients', employees', governors' suppliers', partners' personal data, and any other personal data the school processes from any source.

The policy applies to the processing of personal data wholly or partly by automated means (i.e. by computer), and to the processing other than by automated means of personal data (i.e. paper records) that form part of a filing system, or are intended to form part of a filing system.

The purpose of this Policy and the accompanying Guidance Notes is:

- to explain the requirements of The Stonebridge School under the GDPR and UK relevant legislation
- to make the various parties e.g. teachers and administrators aware of their responsibilities
- to indicate the rights of data subjects

Important: This Policy should be considered in conjunction with the accompanying Guidance Notes and other documents, which are referred to at the end of this Policy. This is because the answers to queries/issues are not always straightforward. If in doubt, contact the school's Data Protection Officer.

3 Policy statement

1. The Stonebridge School, located at Shakespeare Avenue, Stonebridge, London, NW10 8NG & The Stonebridge Annexe at Twybridge Way, Stonebridge, London, NW10 0ST, are committed to compliance with all UK laws in respect of personal data, the protection of the "rights and freedoms" of individuals whose information is collected and processed in accordance with the General Data Protection Regulation (GDPR), and the UK Data Protection Act 2018.
2. The school shall establish all necessary policies, procedures, risk management, training, monitoring, and agreements to ensure that it complies with the GDPR and UK Data Protection Act 2018.
3. The Stonebridge School shall review its compliance with the GDPR and Data Protection Act 2018 on a regular basis.
4. Compliance with the GDPR is described by this policy and other relevant policies such as the Information Security Policy, along with connected processes and procedures.
5. The Data Protection Officer is responsible for reviewing the Record of Processing Activities annually in the light of any changes to The Stonebridge School's activities (as determined by any changes), and to any additional requirements identified by means of data protection impact assessments. This register needs to be available on the Information Commissioner's Office's request.
6. All employees, contractors, governors and business partners, shall pay regard to confidentiality and access to personal information on a need to know basis.
7. Data Protection applies to all employees, contractors, governors and business partners of The Stonebridge School such as outsourced suppliers. Any personal data breach may be dealt with under The Stonebridge School's disciplinary policy, and may also be a criminal offence, in which case the matter will be reported as soon as possible to the Information Commissioner's Office and or appropriate authorities.
8. Partners and any third parties working with or for The Stonebridge School, who have or may have access to personal data, will be expected to have read, understood, and to comply with this policy. No third party may access personal data held by The Stonebridge School without having first entered into a legal agreement, which imposes on the third party obligations no less onerous than those to which The Stonebridge School is committed, and which gives The Stonebridge School the right to audit compliance with the agreement.
9. The school shall follow the related Codes of Practice Guidance issued by the Information Commissioner's Office in relation to Data Protection.

4 Responsibilities

Data protection is the responsibility of all employees to varying degrees. These responsibilities are outlined below:

Senior Management Team – Governors/School Board

The Senior Management Team has overall responsibility and accountability for The Stonebridge School's information, and set the strategic framework through which The Stonebridge School governs Data Protection.

Senior member of staff with responsibility for information (Information Asset Owner)

The responsibilities of the Information Asset Owners are:

- to develop and encourage good information handling practices within their area and their responsibilities are set out in individual job descriptions
- to understand the general requirements and rights of the organisation, managers, and individuals under the GDPR
- to ensure that data protection audits are carried out in their areas on a regular basis
- to ensure that in the light of these audits, any necessary changes to the processing of data are made within the bounds of what is practicable
- to ensure that all school employees complete the mandatory on-line courses
- to ensure that data breaches in their areas are reported promptly, investigated, and risks are reduced

Brent Council Data Protection Service

Brent Council Data Protection Service (school.dpo@brent.gov.uk) supports the Data Protection Officer and is the first point of call for information governance including Data Protection matters.
It is important that any requests for personal information (Subject Access Requests), information sharing arrangements, Privacy/Data Protection Impact Assessments, and any suspected data breaches are notified to the team.

The Data Protection Officer

Data Protection Officer, to co-ordinate The Stonebridge School's compliance with this policy on a day-to-day basis, and in particular has direct responsibility for ensuring that The Stonebridge School's complies with the GDPR, as do senior management in respect of data processing that takes place within their area of responsibility.

The Data Protection Officer has specific responsibilities in respect of procedures such as the Subject Access Request Procedure and are the first point of call for employees seeking clarification on any aspect of data protection compliance.

Reports on a quarterly basis to senior management team for the management of personal data within your school and for ensuring that compliance with data protection legislation and good practice can be demonstrated. This accountability includes:

- development and implementation of the GDPR as required by this policy
- security and risk management in relation to compliance with the policy

The responsibilities of the Data Protection Officer are:

- to promote awareness of the GDPR/data protection throughout the school
- to ensure compliance with the GDPR/data protection throughout the school
- to provide advice and assistance to the school regarding the application of the GDPR
- to update procedures in light of the changes in legislation or guidance from the school senior management team, and to notify the Information Commissioner on an annual basis of all the purposes for which the school processes personal data
- to receive and process all subject access requests together with the maintenance of files required by the Act
- to provide assistance with the training of employees in the provisions of the Act
- to ensure that data is redacted before it is supplied to data subjects under a subject access request
- to ensure that Individual Rights are fulfilled

Managers/Senior Leadership Team

The responsibilities of all managers are:

- to carry out data protection audits in their area on a regular basis
- to inform employees/pupils of the purpose(s) for which their personal data will be used, and who will have access to that data
- to keep personal data up-to-date and accurate

- to allow their employees/pupils access to their personal data through the appropriate mechanisms (see below)
- to ensure that all employees understand the importance of pupil and employees' confidentiality
- to rectify, erase, destroy personal data as per relevant procedures, and the school's records retention policy. All employees should have access to a copy of the Data Protection Policy and guidance notes
- to report potential data breaches to the school's data protection officer immediately, or email school.dpo@brent.gov.uk as soon as there is awareness of a breach or potential breach. This includes awareness of a breach by a third party or supplier
- to carry out data breach investigation relating to their employees

Employees

Compliance with data protection legislation is the responsibility of all employees of the school who process personal data.

The responsibilities of employees are as follows:

- to ensure that personal data remains confidential where appropriate. This includes:
    - not discussing confidential work issues with relatives/ friends
    - turning the screen away from public viewing, not shouting out personal information about customers/other employees across a department/office etc.
    - being careful to whom information is given, especially over the phone
    - ensuring that messages containing personal data left on answer - phones are not overheard by the public
    - using computer passwords/screensavers
    - not disclosing computer passwords
    - logging off the computer when leaving the workstation
    - applying security and confidentiality measures whilst working remotely or from home
- to accurately record information, both manual and computerised
- to comply with a request for information made by the Data Protection Officer
- to make themselves aware of their responsibilities and rights under the GDPR/Data Protection Act. If in doubt, employees should contact their manager or the Data Protection Officer
- to complete the mandatory online course annually
- to report a suspect data breach to their manager, and The Stonebridge School's Designated Data Protection Officer immediately, or email

school.dpo@brent.gov.uk. This should happen as soon as there is awareness of a breach or potential breach

- to ensure that any personal data about them and supplied by them to the school is accurate and up-to-date
- to notify the line manager of any conflict of interest in the data that is to be processed by them or potentially viewed

NB. Individuals can be prosecuted under the GDPR/Data Protection Act, not just the school.

5 The Data Protection Principles

All processing of personal data must be conducted in accordance with the data protection principles as set out in Article 5 of the GDPR. The Stonebridge School's policies and procedures are designed to ensure compliance with the principles.

Personal data must be processed lawfully, fairly, and transparently

Lawful – identify a lawful basis before you can process personal data. These are often referred to as the "conditions for processing", for example consent.

Fairly – in order for processing to be fair, the data controller has to make certain information available to the data subject(s) as practicable. This applies whether the personal data was obtained directly from the data subject(s) or from other sources.

The GDPR has increased requirements about what information should be available to data subjects, which is covered in the 'Transparency' requirement.

Transparently – the GDPR includes rules on giving privacy information to data subjects in Articles 12, 13, and 14. These are detailed and specific, placing an emphasis on making privacy notices understandable and accessible. Information must be communicated to the data subject(s) in an intelligible form using clear and plain language.

The Stonebridge School's Privacy Notices are recorded in the Privacy Notice Register.

The specific information that must be provided to the data subject(s) must, as a minimum, include:

- the identity and the contact details of the controller, and if any, of the controller's representative
- the contact details of the Data Protection Officer
- the purposes of the processing for which the personal data are intended, as well as the legal basis for the processing
- the period for which the personal data will be stored
- the existence of the rights to request access, rectification, erasure, or to object to the processing, and the conditions (or lack of) relating to exercising these rights, such as whether the lawfulness of previous processing will be affected
- the categories of personal data concerned
- the recipients or categories of recipients of the personal data, where applicable
- where applicable, that the controller intends to transfer personal data to a recipient in a third country, and the level of protection afforded to the data (the school does not permit transfer of data to a third country)
- any further information necessary to guarantee fair processing

Personal data can only be collected for specific, explicit, and legitimate purposes

Data obtained for specified purposes must not be used for a purpose that differs from those formally notified to the Information Commissioner's Office as part of The Stonebridge School's GDPR register of processing.

Personal data must be adequate, relevant, and limited to what is necessary for processing

The Data Protection Officer is responsible for ensuring that The Stonebridge School does not collect information that is not strictly necessary for the purpose for which it is obtained.

All data collection forms (electronic or paper-based), including data collection requirements in new information systems, must be included in a fair processing statement, or linked to the privacy statement and approved by the Data Protection Officer.

The Data Protection Officer will ensure that, on an annual basis all data collection methods are reviewed to ensure that collected data continues to be adequate, relevant, and not excessive.

Personal data must be accurate and kept up to date with every effort to erase or rectify without delay

Data that is stored by the data controller must be reviewed and updated as necessary. No data should be kept unless it is reasonable to assume that it is accurate.

The Data Protection Officer is responsible for ensuring that all employees are trained in the importance of collecting accurate data and maintaining it.

It is also the responsibility of the data subject(s) to ensure that data held by The Stonebridge School is accurate and up to date. Completion of a registration or application form by a data subject(s) will include a statement that the data contained therein is accurate at the date of submission.

Employees should be required to notify The Stonebridge School of any changes in circumstance to enable personal records to be updated accordingly. It is the responsibility of The Stonebridge School to ensure that any notification regarding change of circumstances is recorded and acted upon.

The Data Protection Officer is responsible for ensuring that appropriate procedures and policies are in place to keep personal data accurate and up to date, taking into account the volume of data collected, the speed with which it might change, and any other relevant factors.

On at least an annual basis, the Data Protection Officer will review the retention dates of all the personal data processed by The Stonebridge School, by reference to the data inventory, and will identify any data that is no longer required in the context of the

registered purpose. This data will be securely deleted/destroyed in line with the Secure Disposal of Storage Media Procedure.

The Data Protection Officer is responsible for responding to requests for rectification from data subject(s) within one month. This can be extended to a further two months for complex requests. If The Stonebridge School decides not to comply with the request, the Data Protection Officer must respond to the data subject(s) to explain its reasoning, and inform them of their right to complain to the Information Commissioner's Office and seek judicial remedy.

The Data Protection Officer is responsible for making appropriate arrangements that, where third-party organisations may have been passed inaccurate or out-of-date personal data, to inform them that the information is inaccurate and/or out of date and is not to be used to inform decisions about the individuals concerned; and for passing any correction to the personal data to the third party where this is required.

Personal data must be kept in a form such that the data subject can be identified only as long as is necessary for processing

Where personal data is retained beyond the processing date, it will be minimised/encrypted/pseudonymised in order to protect the identity of the data subject in the event of a data breach.

Personal data will be retained in line with the Records Retention Policy and, once its retention date is passed, it must be securely destroyed as set out in this procedure.

The Data Protection Officer must specifically approve any data retention that exceeds the retention periods defined in Records Retention Policy, must ensure that the justification is clearly identified and in line with the requirements of the data protection legislation. This approval must be in writing.

Personal data must be processed in a manner that ensures the appropriate security

The Data Protection Officer will carry out a risk assessment taking into account all the circumstances of The Stonebridge School's controlling or processing operations.

In determining appropriateness, the Data Protection Officer should also consider the extent of possible damage or loss that might be caused to individuals (e.g. employees or pupils) if a security breach occurs, the effect of any security breach on The Stonebridge School itself, and any likely reputational damage including the possible loss of public trust.

When assessing appropriate technical measures, the Data Protection Officer will consider the following:

- Compliance with technical standards, including;
- The Payment Card Industry Standards
- The Cloud Security Principles for third parties and suppliers

- The security standards defined by the National Cyber Security Centre
- Password protection
- Automatic locking of idle terminals
- Removal of access rights for USB and other memory media
- Virus checking software and firewalls
- Role-based access rights including those assigned to temporary employees
- Encryption of devices that leave the organisations premises such as laptops
- Security of local and wide area networks
- Privacy enhancing technologies such as pseudonymisation and anonymisation
- Identifying appropriate international security standards relevant to The Stonebridge School

When assessing appropriate organisational measures, the Data Protection Officer will consider the following:

- The appropriate training levels throughout The Stonebridge School
- Measures that consider the reliability of employees (such as references etc.)
- The inclusion of data protection in employment contracts
- Identification of disciplinary action measures for data breaches
- Monitoring of employees for compliance with relevant security standards
- Physical access controls to electronic and paper based records
- Adoption of a clear desk policy
- Storing of paper based data in lockable fire-proof cabinets
- Restricting the use of portable electronic devices outside of the workplace
- Restricting the use of employee's own personal devices being used in the workplace
- Adopting clear rules about passwords
- Making regular backups of personal data and storing the media off-site
- The imposition of contractual obligations on the importing organisations to take appropriate security measures when transferring data outside the EEA. However, the current position is that transfer of data to third countries is prohibited, without explicit temporary approval from the Data Protection Officer
- Follow guidelines set out in the Acceptable User Policy (AUP).

These controls have been selected on the basis of identified risks to personal data, and the potential for damage or distress to individuals whose data is being processed.

The controller must be able to demonstrate compliance with the GDPR's other principles (accountability)

The GDPR includes provisions that promote accountability and governance. These complement the GDPR's transparency requirements. The accountability principle in Article 5(2) requires you to demonstrate that you comply with the principles, and states explicitly that this is your responsibility.

The Stonebridge School will demonstrate compliance with the data protection principles by implementing data protection policies, adhering to codes of conduct, implementing technical and organisational measures, as well as adopting techniques such as data protection by design, DPIAs, breach notification procedures, and incident response plans.

6 Data subject(s)' rights

Data subject(s) have the following rights regarding data processing, and the data that is recorded about them:

- To make subject access requests regarding the nature of information held and to whom it has been disclosed
- To prevent processing likely to cause damage or distress
- To prevent processing for purposes of direct marketing
- To be informed about the mechanics of automated decision-taking process that will significantly affect them
- To not have significant decisions that will affect them taken solely by automated process
- To sue for compensation if they suffer damage by any contravention of the GDPR
- To take action to rectify, block, erased, including the right to be forgotten, or destroy inaccurate data
- To request the supervisory authority to assess whether any provision of the GDPR has been contravened
- To have personal data provided to them in a structured, commonly used, machine-readable format, and the right to have that data transmitted to another controller
- To object to any automated profiling that is occurring without consent

The Stonebridge School ensures that data subjects may exercise these rights:

- Data subject(s) may make data access requests as described in Subject Access Request Procedure; this procedure also describes how The Stonebridge School will ensure that its response to the data access request complies with the requirements of the GDPR
- Data subject(s) have the right to complain to The Stonebridge School relating to the processing of their personal data, the handling of a request from a data subject(s), and appeals from a data subject on how complaints have been handled in line with the Data Protection Complaints Procedure

7 Consent

7.1 The Stonebridge School understands 'consent' to mean that it has been explicitly and freely given, and a specific, informed and unambiguous indication of the data subject(s) wishes that, by statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. The data subject can withdraw their consent at any time.

7.2 The Stonebridge School understands 'consent' to mean that the data subject has been fully informed of the intended processing and has signified their agreement, while in a fit state of mind to do so and without pressure being exerted upon them. Consent obtained under duress or on the basis of misleading information will not be a valid basis for processing.

7.3 There must be some active communication between the parties to demonstrate active consent. Consent cannot be inferred from non-response to a communication. The Stonebridge School must be able to demonstrate that consent was obtained for the processing operation.

7.4 For sensitive data, explicit written consent of data subjects must be obtained unless an alternative legitimate basis for processing exists.

7.5 In most instances, consent to process personal and sensitive data is obtained routinely by The Stonebridge School using standard consent documents e.g. when a new client signs a contract, or during induction for participants on programmes.

7.6 Where The Stonebridge School provides online services to children, parental or custodial authorisation must be obtained. This requirement applies to children under the age of 13.

8 Security of data

8.1 All employees /partners/suppliers are responsible for ensuring that any personal data that The Stonebridge School holds for which they are responsible, is kept securely, and is not under any conditions disclosed to any third party unless that third party has been specifically authorised by The Stonebridge School to receive that information and has entered into a confidentiality agreement.

8.2 All personal data should be accessible only to those who need to use it, and access may only be granted in line with the Access Control Policy. All personal data should be treated with the highest security and must be kept:

- in a lockable room with controlled access
- in a locked drawer or filing cabinet
- if computerised, password protected in line with corporate requirements in the Access Control Policy
- stored on (removable) computer media which are encrypted in line with Secure Disposal of Storage Media

8.3 Care must be taken to ensure that PC screens and terminals are not visible except to authorised employees of The Stonebridge School. All employees are required to read and accept the Acceptable Use Policy before they are given access to organisational information of any sort, which details rules on screen time-outs.

8.4 Manual records may not be left where they can be accessed by unauthorised personnel, and may not be removed from business premises without explicit authorisation. As soon as manual records are no longer required for day-to-day client

support, they must be removed from secure archiving in line with Records Retention and Disposal Policy.

8.5 Personal data may only be deleted or disposed of in line with Records Retention Policy. Manual records that have reached their retention date are to be shredded and disposed of as 'confidential waste'. Hard drives of redundant PCs are to be removed and immediately destroyed as required by before disposal.

8.6 Processing of personal data 'off-site' presents a potentially greater risk of loss, theft or damage to personal data. Employees must be specifically authorised to process data off-site.

9 Disclosure of data

The Stonebridge School must ensure that personal data is not disclosed to unauthorised third parties which includes family members, friends, government bodies, and in certain circumstances, the Police. All employees should exercise caution when asked to disclose personal data held on another individual to a third party and request the third party to complete a DS1 Disclosure of third party personal information form. It is important to bear in mind whether or not disclosure of the information is relevant to, and necessary for the conduct of' The Stonebridge School's business.
All requests to provide data for one of these reasons must be supported by appropriate paperwork, and all such disclosures must be specifically authorised by the Data Protection Officer.

10 Retention and disposal of data

The Stonebridge School shall not keep personal data in a form that permits identification of data subjects(s) for longer a period than is necessary, in relation to the purpose(s) for which the data was originally collected.
The Stonebridge School may store data for longer periods if the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the implementation of appropriate technical and organisational measures to safeguard the rights and freedoms of the data subject(s).
The retention period for each category of personal data will be set out in the Records Retention Policy along with the criteria used to determine this period including any statutory obligations The Stonebridge School has to retain the data.
The Stonebridge School's Records Retention Policy will apply in all cases.
Personal data must be disposed of securely in accordance with the sixth principle of the GDPR – processed in an appropriate manner to maintain security, thereby protecting the "rights and freedoms" of data subject(s). Any disposal of data will be done in accordance with the secure disposal procedure.

11 Data transfers

All exports of data from within the European Economic Area (EEA) to non-European Economic Area countries (referred to in the GDPR as 'third countries') are unlawful unless there is an appropriate "level of protection for the fundamental rights of the data subjects". The transfer of personal data outside of the EEA is prohibited. Any exemptions shall be approved by the Data Protection Officer.

12 Record of Processing Activities (RoPA)

The Stonebridge School's has established a data inventory and data flow process as part of its approach to address risks and opportunities throughout its GDPR compliance project. The Stonebridge School's data inventory and data flow determines:

- business processes that use personal data
- source of personal data
- volume of data subject(s)
- description of each item of personal data
- processing activity
- maintains the inventory of data categories of personal data processed
- documents the purpose(s) for which each category of personal data is used
- recipients, and potential recipients of the personal data
- the role of the school throughout the data flow
- key systems and repositories
- any data transfers; and
- all retention and disposal requirements

The Stonebridge School is aware of any risks associated with the processing of particular types of personal data:

- The Stonebridge School assesses the level of risk to individuals associated with the processing of their personal data. Data protection impact assessments (DPIAs) (DPIA Procedure) are carried out in relation to the processing of personal data by The Stonebridge School, and in relation to processing undertaken by other organisations on behalf of The Stonebridge School
- The Stonebridge School shall manage any risks identified by the risk assessment in order to reduce the likelihood of a non-conformance with this policy
- Where a type of processing, in particular using new technologies and taking into account the nature, scope, context, and purposes of the processing is likely to result in a high risk to the rights and freedoms of natural persons. The Stonebridge School shall, prior to the processing, carry out a DPIA of the impact of the envisaged processing operations on the protection of personal data. A single DPIA may address a set of similar processing operations that present similar high risks.
- Where, as a result of a DPIA it is clear that The Stonebridge School is about to commence processing of personal data that could cause damage and/or distress

to the data subjects, the decision as to whether or not The Stonebridge School may proceed must be escalated for review to the Data Protection Officer
- The Data Protection Officer shall, if there are significant concerns, either as to the potential damage or distress, or the quantity of data concerned, escalate the matter to the Information Commissioner's Office
- Appropriate controls will be selected and applied to reduce the level of risk associated with processing individual data to an acceptable level, by reference to The Stonebridge School's documented risk acceptance criteria and the requirements of the GDPR

13 Data breaches

The school (the data controller) must keep a log of data breaches relating to personal and sensitive information and notify the Information Commissioner in accordance with their guidance and within 72 hours.

When the school or its provider/supplier becomes aware of a data breach or potential breach, it must report it to the Data Protection Officer immediately. If this is not reported immediately, the person or area that became aware must provide written justification for any delay.

14 Concerns about data protection

Any queries or concerns about data protection shall be addressed by the data protection officer and/or Data Protection Service.

Should individuals be dissatisfied with the responses from the Data Protection Officer and/or the Data Protection Service, they will be directed to the Information Commissioner's Office to conduct an assessment.

15 Further information

Reference to other policies documents

The following documents provide further details/ guidelines on data protection in this School.

These documents are:

- Access Control Policy
- Acceptable Use Policy
- Records Retention Policy

Further information/advice

Further information/advice on Data Protection are available from:

- The school's Data Protection Officer, ext. 2018, school.dpo@brent.gov.uk
- The Legal Services
- Your line manager

Appendix 1 – Glossary of Terms

Article 4 definitions

Establishment – the main establishment of the controller in the EU will be the place in which the controller makes the main decisions as to the purpose and means of its data processing activities. The main establishment of a processor in the EU will be its administrative centre. If a controller is based outside the EU, it will have to appoint a representative in the jurisdiction in which the controller operates to act on behalf of the controller and deal with supervisory authorities.

Personal data – any information relating to an identified or identifiable natural person ('data subject(s'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

Special categories of personal data – 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.

Data controller – the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

Data subject – any living individual who is the subject of personal data held by an organisation.

Processing – any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Profiling – is any form of automated processing of personal data intended to evaluate certain personal aspects relating to a natural person, or to analyse or predict that person's performance at work, economic situation, location, health, personal preferences, reliability, or behaviour. This definition is linked to the right of the data subject to object to profiling and a right to be informed about the existence of profiling, of measures based on profiling and the envisaged effects of profiling on the individual.

Personal data breach – a breach of security leading to the accidental, or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data transmitted, stored or otherwise processed. There is an obligation on the controller to report personal data breaches to the Information Commissioner's Office, and where the breach is likely to adversely affect the personal data or privacy of the data subject(s).

Data subject consent - means any freely given, specific, informed, and unambiguous indication of the data subject(s) wishes by which he or she by a statement or by a clear affirmative action, signifies agreement to the processing of personal data.

Child – the GDPR defines a child as anyone under the age of 16 years old, although this may be lowered to 13 by Member State law. The processing of personal data of a child is only lawful if parental or custodian consent has been obtained. The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child.

Third party – a natural or legal person, public authority, agency or body other than the data subject(s), controller, processor, and persons who under the direct authority of the controller or processor, are authorised to process personal data.

Filing system – any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised, or dispersed on a functional or geographical basis.