ST. BARTHOLOMEW'S SCHOOL
DATA PROTECTION POLICY

Agreed by the Finance & Risk Committee Summer 2019
Approved by the Full Governing Body Summer 2019
To be reviewed Summer 2020

Purpose: It is the responsibility of Governors to make sure that procedures are in place to ensure that the Academy complies with the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679).

Contents:

1. Introduction

This Data Protection Policy sets out how St Bartholomew's School ("we", "us", "Academy", "Academy Trust" and "the School") of Andover Road, Newbury, Berkshire, RG14 6JP, handles the personally identifiable information relating to those individuals with whom we have a relationship.

St Bartholomew's School is committed to ensuring all personal information is properly managed and that it is compliant with the GDPR. The School will make every effort to meet its obligations under the legislation and will regularly review procedures to ensure that it is doing so.

2. Scope

This Data Protection Policy sets out our data protection standards to comply with the GDPR and details how we handle the Personal Data of all those living individuals with whom we have a relationship. These individuals include students, staff (prospective employees, current and previous staff, and temporary staff), governors, visitors and suppliers (contractors, agents and representatives).

This policy applies to all personal information created or held by the School in whatever format (for example, paper, electronic, email, microfiche, film, audio, images) and however it is stored, (for example, ICT system/database, shared drive filing structure, email, filing cabinet, shelving and personal filing drawers).

GDPR definitions are detailed in **Appendix 1.**

3. Responsibilities

St Bartholomew's School is the Data Controller.

The Governing Body have overall accountability for compliance with the GDPR.

The Headteacher is responsible for ensuring compliance with the GDPR and this policy within the day to day activities of the School. This responsibility is delegated to the Data Protection Officer (DPO).

The Data Protection Officer role has delegated responsibility for GDPR compliance. The DPO is answerable to the Governors for the management of personal information within the School and for ensuring that compliance with all data protection legislation. The role and responsibilities of the DPO are detailed in **Appendix 2.**

All individuals who process Personal Data on behalf of the School are responsible for compliance with the GDPR and must ensure that personal information is processed in-line with the GDPR and this Policy.

4. GDPR Requirements

We adhere to the principles relating to Processing of Personal Data set out in the GDPR which require Personal Data to be:

(a) Processed lawfully, fairly and in a transparent manner (Lawfulness, Fairness and Transparency).
(b) Collected only for specified, explicit and legitimate purposes (Purpose Limitation).
(c) Adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed (Data Minimisation).
(d) Accurate and where necessary kept up to date (Accuracy).
(e) Not kept in a form which permits identification of Data Subjects for longer than is necessary for the purposes for which the data is Processed (Retention or Storage Limitation).
(f) Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful Processing and against accidental loss, destruction or damage (Security, Integrity and Confidentiality).
(g) Not transferred to another country without appropriate safeguards being in place (Transfer Limitation).
(h) Made available to Data Subjects and Data Subjects allowed to exercise certain rights in relation to their Personal Data (Data Subject's Rights and Requests).

We are responsible for and must be able to demonstrate compliance with the data protection principles listed above (Accountability).

5. Notification

Under the GDPR, St Bartholomew's School as a data controller pays an annual fee to the ICO. St Bartholomew's School is no longer required to register with the ICO (previous registration number for the School is Z581823X). This is replaced with the requirement to comply with the Accountability principle of maintaining a detailed record of its processing activities (the data processing register).

6. Lawfulness, fairness and transparency

6.1 Lawfulness and fairness

We only collect, process and share personal data fairly and lawfully and for specified purposes. The GDPR restricts our actions regarding personal data to specified lawful purposes. These restrictions are not intended to prevent processing but ensure that we process personal data fairly and without adversely affecting the data subject.

All processing must be justified by a clear lawful basis, with additional obligations applicable to the processing of special categories of personal data (this includes data relating to health, biometrics). These legal bases are summarised in **Appendix 3** and documented in our **Data Processing Register**.

In summary:

For student and parent data (where the task is specified in law i.e. education):

- Our main legal basis is that it is "necessary in the public interest" (for example, to provide students with an education);
- Some processing may rely upon a legal obligation (for example, to report to parents annually);
- And on occasions, we rely on consent:
    - This is only used where there is no other relevant basis, and the data subject has a genuine choice, so the consent is freely given (for example, to share contact details with the Parents' Association; for student photographs * for use in school materials; or for alumni communications);
    - But is required from a child aged 13 and over, and sufficiently competent to process data in regard to information society services (online services) unless this is part of the public interest task;
    - And always for explicit consent for the processing of special categories of data (for example, in support of health data required for school trips or biometrics for cash-free catering).
    - Photographs taken of individual students for School use (for example, to use on our website or in other media) will be on the basis of explicit consent from each individual;

*Photographs taken by students and parents for personal use are outside GDPR and so are permitted;

For data relating to other data subjects (non-students) (i.e. where the task is not specified by law):

- Processing may be necessary for the performance of a contract to which the data subject is a party (being the employment contract);
- Some processing may be necessary for compliance with a legal obligation to which St Bartholomew's School, as data controller, is subject (for example, collecting PAYE payments);
- As a legitimate interest of the School (for example, network security and CCTV);
- To assess the working capacity of our employees.

We identify and document in our Data Processing Register the legal ground being relied on for each Processing activity - the Register is reviewed on an ongoing basis.

The legal bases are summarised in the Privacy Notices provided to our data subjects (e.g. to staff; to students).

6.2 Privacy Notice (Transparency)

Whenever information is collected about individuals they are referred to an appropriate Privacy Notice at the time that information is first processed. The Notice must be concise, transparent, easily accessible and use clear and plain language, detailing:

- Our identity as the data controller, e.g. the School;
- The purpose that the information is being collected for;
- Any other purposes that it may be used for;
- Who the information will or may be shared with;
- How we protect and retain that Personal Data;
- How to contact the data controller; and
- How to make a complaint to the Information Commissioner's Office (ICO).

7. **Purpose limitation**

We use personal data only for the reasons provided in the Privacy Notice/s, and we do not use Personal Data for new, different or incompatible purposes from that disclosed when it was first obtained unless we have informed the Data Subject of the new purposes and they Consent where necessary.

8. **Data minimisation**

We only allow employees or other authorised parties to Process Personal Data when performing their duties as instructed and not for any reason unrelated to those stated duties.
We do not collect excessive data and ensure any Personal Data collected is adequate and relevant for the intended purposes.
We ensure that when Personal Data is no longer needed for specified purposes, it is deleted (or anonymised) in accordance with the Records and Data Retention Policy.

9. **Accuracy of data**

We ensure that the Personal Data we use and hold is accurate, complete, kept up to date and relevant to the purpose for which we collected it. We check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards. We take all reasonable steps to destroy or amend inaccurate or out-of-date Personal Data.

We ensure that records are kept in such a way that the individual or other authorised parties can inspect them and must be correct, unbiased, unambiguous and clearly decipherable/readable.

Where information is obtained from an outside source, details of the source and date obtained should be recorded.

Any person whose details, or child's details, are to be included on the School's website will be required to give written consent. At the time the information is included all such individuals will be properly informed about the consequences of their data being disseminated worldwide.

10. **Data Retention (Storage limitation)**

We do not keep Personal Data in a form which permits the identification of the Data Subject for longer than needed for the purposes for which we originally collected it including for the purpose of satisfying any legal, accounting or reporting requirements.

We maintain retention policies and procedures to ensure Personal Data is deleted after a reasonable time for the purposes for which it was being held, unless a law requires such data to be kept for a minimum time. We take all reasonable steps to destroy or erase from our systems all Personal Data that we no longer require; this includes requiring third parties to delete such data where applicable.

Most personal information is retained for the period during which the person is associated with the School plus an additional period which the School has determined or as required by law.

These standards and retention periods are detailed in the **Records and Data Retention Policy and Schedule.**

11. Security integrity and confidentiality

11.1 Protecting Personal Data

We develop, implement and maintain appropriate technical and organisational security measures in order to protect the Personal Data we hold, to protect against unlawful or unauthorised Processing and against the accidental loss of, or damage to, Personal Data.

This includes ensuring:

- Confidentiality of personal data - so that only people who have a need to know and are authorised to use the Personal Data can access it.
- Integrity of Personal Data - so it is accurate and suitable for the purpose for which it is processed.

- Availability of personal data – so that authorised users are able to access the Personal Data when they need it for authorised purposes.
- Procedures and technologies that maintain the security of all Personal Data from the point of collection to the point of destruction
- The evaluation and testing the effectiveness of those safeguards to ensure security of our Processing of Personal Data.
- That transfers of Personal Data to third-party service providers take place only with written agreement to comply with our policies and procedures.

These standards are detailed in the **Information Security Policy.**

11.2 Sharing Personal Data

Relevant, confidential data should only be shared or disclosed to:

- Other members of staff on a need to know basis;
- Relevant Parents/Guardians;
- Other authorities, such as the LA and Colleges to which a student may move;
- Other organisations that provide us and our students with relevant services, such as Youth Support Services, careers services, post-16 education and training providers, university and apprenticeship application services;
- Our Parents' Association (where consent has been given) so it can improve links between students, parents and staff and raise funds to support education at St Bartholomew's School;
- Third party organisation that provide us with contracted services (such as our payroll provider) and on the basis of a written contract and/or specification that contains GDPR approved third party clauses;
- Other authorities if it is necessary in the public interest, such as the Police for the prevention of crime;

Sharing Personal Data should comply with Fair Processing and the Privacy Notice and, if required, the Data Subject's Consent has been obtained.

The School should not disclose anything on a student's record which would be likely to cause serious harm to their physical or mental health or that of anyone else. Therefore, those who create such records should ensure that such information is separated from other records.

Third party data (information about someone other than the requesting individual) should in general only be provided with the consent of the individual in question. When giving information to an individual, particularly by telephone, it is most important that the individual's identity is verified. If in doubt, questions should be asked of the individual, to which only he/she is likely to know the answers. Information should not be provided to other parties, even if related. For example: in the case of divorced parents it is important that information regarding one party is not given to the other party to which he/she is not entitled.

11.3 **Reporting a Personal Data Breach**

We have put in place procedures to deal with any suspected Personal Data Breach and will notify Data Subjects or any applicable regulator where we are legally required to do so. The DPO is responsible for managing the data breach and can be contacted at: DPO@stbarts.co.uk

These standards are detailed in the **Data Breach Policy.**

12. **Transferring Personal Data**

12.1 We endeavour to only process personal information within the EEA

12.2 Where this is not possible, we only transfer Personal Data outside the EEA if one of the following conditions applies:

(a) The European Commission has issued a decision confirming that the country to which we transfer the Personal Data ensures an adequate level of protection for the Data Subjects' rights and freedoms;
(b) Appropriate safeguards are in place such as binding corporate rules (BCR), standard contractual clauses approved by the European Commission, an approved code of conduct or a certification mechanism, a copy of which can be obtained from the DPO;
(c) The Data Subject has provided Explicit Consent to the proposed transfer after being informed of any potential risks; or
(d) The transfer is necessary for one of the other reasons set out in the GDPR including the performance of a contract between us and the Data Subject, reasons of public interest, to establish, exercise or defend legal claims or to protect the vital interests of the Data Subject where the Data Subject is physically or legally incapable of giving Consent and, in some limited cases, for our legitimate interest.

12.3 We transfer personal data to countries outside the EEA relating to the management of school trips, for example to China, Morocco or the USA. Where we do so, we seek explicit consent to do so from the individual (this may be the student, the parent or carer, and the member of staff) and put in place adequate security to protect that data.

12.4 Individuals may choose to sign-up to other services, sites or applications as part of their educational experience. Doing so is not a School requirement and we are not responsible for the privacy policies and/or practices from other organisations; our Privacy Notices require that individuals should read all third parties' privacy policies before sharing their data.

13. Data Subject's rights and requests

All our Data Subjects, whether staff, students or others, have rights when it comes to how we handle their Personal Data. These include rights:

i. To be informed – all organisations must be completely transparent in how they are using personal data (personal data may include data such as a work email and work mobile telephone if they are specific to an individual).
ii. Of access - individuals will have the right to know exactly what information is held about them and how it is processed. This is commonly known as a "**data subject access request"** (DSAR). This enables the individual to receive a copy of the personal information we hold about them and to check that we are lawfully processing it.

When a DSAR is received it must be dealt with as a priority and escalated to the DPO as a response must be provided with one month and at no charge;

iii. Of rectification - individuals will be entitled to have personal data rectified if it is inaccurate or incomplete;
iv. To erasure - also known as 'the right to be forgotten', this refers to an individual's right to having their personal data deleted or removed without the need for a specific reason as to why they wish to discontinue.
v. To restrict processing - an individual's right to block or suppress processing of their personal data;
vi. To data portability - this allows individuals to retain and reuse their personal data for their own purpose, but only on the basis of consent;
vii. To object - in certain circumstances, individuals are entitled to object to their personal data being used. This includes, if an organisation uses personal data for the purpose of direct marketing, scientific and historical research, or for the performance of a task in the public interest;
viii. Of automated decision making and profiling - the GDPR puts in place safeguards to protect individuals against the risk that a potentially damaging decision is made without human intervention. For example, individuals can choose not to be the subject of a decision where the consequence has a legal bearing on them, or is based on automated processing.

Children's Data Protection Rights
Children over the age of 13, and those considered sufficiently competent, can exercise their own data protection rights. If the child does not appear to understand the nature of the request, someone with parental responsibility for the child, or a guardian, is entitled to make the request on behalf of the child and receive a response.

Parents' and Carers' Data Protection Rights
An adult with parental responsibility can access the information about their child, as long as the child is not considered to be sufficiently mature. They must be able to prove their parental responsibility and the School is entitled to request relevant documentation to evidence this as well as the identity of the requestor and child.

These standards are detailed in the **Rights and Requests (DSAR) Policy**.

14. Accountability

14.1 We are responsible for, and must be able to demonstrate, compliance with the data protection principles.

This includes:
(a) A Data Protection Officer to deal with data privacy;
(b) Implementing Privacy by Design when Processing Personal Data and completing Data Protection Impact Assessments (DPIA) where Processing presents a high risk to rights and freedoms of Data Subjects;
(c) Integrating data protection into internal documents;
(d) Training staff on the GDPR, this Data Protection Policy and any related policies and procedures, and maintaining a record of training attendance by staff; and
(e) Regularly testing the privacy measures implemented and conducting periodic reviews and audits to assess compliance, including using results of testing to demonstrate compliance improvement effort.

14.2 Record keeping

We keep and maintain accurate records reflecting our Processing, including records of Data Subjects' Consents and procedures for obtaining Consents.

The Data Processing Register includes the name and contact details of the Data Controller and the DPO, clear descriptions of the Personal Data types, Data Subject types, Processing activities, Processing purposes, third-party recipients of the Personal Data, Personal Data storage locations, Personal Data transfers, the Personal Data's retention period and a description of the security measures in place.
This is informed by data maps that include the detail set out above together with appropriate data flows.

14.3 Training and audit

We ensure all staff have undergone training to enable them to comply with data privacy laws. This is mandatory training and is refreshed regularly and recorded.
We regularly review all the systems and processes under our control to ensure they comply with this Data Protection Policy and check that adequate governance controls and resources are in place to ensure proper use and protection of Personal Data.

14.4 Privacy By Design and Data Protection Impact Assessment (DPIA)

We conduct DPIA's in respect to high risk Processing, such as when implementing major system change programs involving the Processing of Personal Data including the use of new or changing technologies (programs, systems or processes); large scale Processing of Sensitive Data; and large scale, systematic monitoring of a publicly accessible area.

This approach is documented in the **DPIA Procedure.**

14.5 Automated Processing (including profiling) and Automated Decision-Making

The School does not carry out any automated processing.

15. Breach of the policy

Failure to comply with this Policy and associated policies (e.g. Data protection or Information Security) puts personal data at risk. Employees may be liable to disciplinary action if they fail to comply with the provisions of this, and all related policies and procedures.

Other parties who act in breach of this Policy, or who do not act to implement it, may be subject to other appropriate sanctions.

16. Policy Management.

Publication - This policy shall be available through the DPO and will be placed on the School's website

Revisions - The DPO is responsible for the maintenance and accuracy of this policy. This Policy will be reviewed on an annual basis and approved by Governors.

Other Documents and Policies - this Data Protection Policy is supported by other policies identified throughout, including:

i. The Information Security Policy
ii. Staff Guidance
    - ICT Instructions for New Staff
    - Rules for Responsible Computer and Internet Use (Students)
    - Staff Acceptable Use Policy (IT Systems and Data)
    - Staff Handbook
    - Staff Privacy Notice
iii. Student Privacy Notice
iv. Parents Handbook
v. The Records and Data Retention Policy and Schedule
vi. The Rights and Requests (DSAR) Policy
vii. The Data Breach Policy
viii. Data Protection Impact Assessment (DPIA) Procedure
ix. CCTV Policy
x. Data Processing Register

....

Signed by Chair of Governors Date

Appendix – GDPR Definitions

Automated Decision-Making (ADM): when a decision is made which is based solely on Automated Processing (including profiling) which produces legal effects or significantly affects an individual. The GDPR prohibits Automated Decision-Making (unless certain conditions are met) but not Automated Processing.

Automated Processing: any form of automated processing of Personal Data consisting of the use of Personal Data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. Profiling is an example of Automated Processing.

School Personnel: all employees, workers, contractors, agency workers, consultants, directors, Members, trustees, governors and others.

Consent: agreement which must be freely given, specific, informed and be an unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear positive action, signify agreement to the Processing of Personal Data relating to them.

Data Controller: the person or organisation that determines when, why and how to process Personal Data. It is responsible for establishing practices and policies in line with the GDPR. We are the Data Controller of all Personal Data relating to our School Personnel, students and others whose data we process.

Data Processor: A natural or legal person, Public Authority, Agency or other body which Processes Personal Data on behalf of a Data Controller.

Data Protection - The process of safeguarding Personal Data from unauthorised or unlawful disclosure, access, alteration, processing, transfer or destruction.

Data Subject: a living, identified or identifiable individual about whom we hold Personal Data. Data Subjects may be nationals or residents of any country and may have legal rights regarding their Personal Data.

Data Privacy Impact Assessment (DPIA): tools and assessments used by the School to identify and reduce risks of a data processing activity.

Data Protection Officer (DPO): the individual with responsibility for Data Protection compliance.

Educational Record: The educational record is confined to information that comes from a teacher or other employee of the school, the student or their parents. Communications about a particular child from head teachers and teachers and other employees at a local authority will therefore form part of that child's official educational record, as will correspondence from an educational psychologist engaged by the governing body under a contract of services. It may also include information from the child and their parents, such as information about the health of the child. Information kept by a teacher solely for their own use does not form part of the official educational record.

EEA: the 28 countries in the EU, and Iceland, Liechtenstein and Norway.

Employee - An individual who works part-time or full-time for the School under a contract of employment, whether oral or written, express or implied, and has recognized rights and duties. Includes temporary employees, trainees, interns, volunteers, governors, temporary and agency workers, and independent contractors.

Explicit Consent: consent which requires a very clear and specific statement (that is, not just action).

Freedom of Information Act 2000 (FoIA) - The Freedom of Information Act 2000 (c.36) is an Act of Parliament of the Parliament of the United Kingdom that creates a public "right of access" to information held by public authorities. It is the implementation of freedom of information legislation in the United Kingdom on a national level.

General Data Protection Regulation (GDPR): The General Data Protection Regulation (*(EU) 2016/679*). Personal Data is subject to the legal safeguards specified in the GDPR.

Information Commissioner (Office) - the Authority responsible for UK Data Protection regulation

Personal Data: any information identifying a Data Subject or information relating to a Data Subject that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. Personal Data includes Sensitive Personal Data and Pseudonymised Personal Data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

Personal Data Breach: any act or omission that compromises the security, confidentiality, integrity or availability of Personal Data or the physical, technical, administrative or organisational safeguards that we or our third-party service providers put in place to protect it. The loss, or unauthorised access, disclosure or acquisition, of Personal Data is a Personal Data Breach.

Privacy by Design: implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the GDPR.

Privacy Notices (also referred to as Privacy Policy) or Privacy Policies: separate notices setting out information that may be provided to Data Subjects when the School collects information about them. These notices may take the form of general privacy statements applicable to a specific group of individuals (for example, employee privacy notices or the website privacy policy) or they may be stand-alone, one-time privacy statements covering Processing related to a specific purpose.

Processing or Process: any activity that involves the use of Personal Data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring Personal Data to third parties.

Pseudonymisation or Pseudonymised: replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person, to whom the data relates, cannot be identified without the use of additional information which is meant to be kept separately and secure.

Special Category Personal Data: information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data, and Personal Data relating to criminal offences and

convictions.

Third party - an external organisation with which St Bartholomew's School conducts business and is also authorised to, under the direct authority of St Bartholomew's School, process personal data of St Bartholomew's School records. This includes any third party that is a natural or legal person, public authority, agency or body (other than the St Bartholomew's School and its data subjects).

Appendix 2 – The Role of the Data Protection Officer

The GDPR outlines three circumstances when an organisation must appoint a Data Protection Officer (DPO) if you:

1. are a *public authority* (except for courts acting in their judicial capacity);
2. carry out large scale systematic monitoring of individuals (for example, online behaviour tracking); or
3. carry out large scale processing of special categories of data or data relating to criminal convictions and offences.

As a public authority, circumstance 1 applies to maintained schools and academies, meaning that St Bartholomew's School needs to name a DPO.

The tasks of the DPO

The DPO takes an advisory and monitoring role and should guide the school to be GDPR compliant.

The DPO's minimum tasks are defined in GDPR Article 39:

- To inform and advise the organisation and its employees about their obligations to comply with the GDPR and other data protection laws.
- To monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments; train staff and conduct internal audits.
- To be the first point of contact for supervisory authorities (the ICO) and for individuals whose data is processed (employees, customers etc).

DPO responsibilities

- Educating the school and its staff on important compliance requirements
- Training staff involved in data processing
- Conducting audits to ensure compliance and address potential issues proactively
- Serving as the point of contact between the school and GDPR Supervisory Authorities
- Monitoring performance and providing advice on the impact of data protection efforts
- Maintaining comprehensive records of all data processing activities
- Interconnecting with data subjects or parents to inform them about: how their data is being used; their rights to have their, or their child's personal data erased; the measures in place to protect their, or their child's, personal information.

Who can be the DPO?

The DPO may be a member of staff or someone from an outside organisation – there are no formal qualifications required for the role however the DPO must meet certain criteria.

As a school, St Bartholomew's School ensures that:

- The DPO reports to the highest management level of the school, i.e. the Governing Body.
- The DPO operates independently and is not dismissed or penalised for performing their task.
- Adequate resources are provided to the enable DPO to meet their GDPR obligations.

The DPO role is impartial, reports directly to the Governing Body and can have no conflict of interest in their other duties.

Qualifications for the DPO

The GDPR does not specify the relevant qualifications that DPOs need, but it does require a DPO to have “expert knowledge of data protection law and practices.”

DPOs may be a staff member and related organisations may use the same individual to oversee data protection collectively, provided that it is possible for all data protection activities to be managed effectively.

It is required that the DPO’s contact details are released publicly and provided to all regulatory oversight agencies.

Appendix 3 – Lawful Basis for Processing

The lawful bases for processing are set out in Article 6 of the GDPR.

At least one of these must apply when processing personal data:

(a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose.
(b) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.
(c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).
(d) Vital interests: the processing is necessary to protect someone's life.
(e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
(f) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

Special Categories of data include information about an individual's: race; ethnic origin; politics; religion; trade union membership; genetics; biometrics (where used for ID purposes); health; sex life; or sexual orientation.
This special data requires more protection so must also satisfy an additional specific condition where the processing is necessary:

a) with explicit consent to the processing of those personal data for one or more specified purposes;
(b) to carry out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law;
(c) to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
(d) for its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim;
(e) to personal data which are manifestly made public by the data subject;
(f) for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
(g) for reasons of substantial public interest;
(h) for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services;
(i) for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices;
(j) for archiving purposes in the public interest, scientific or historical research purposes or statistical.