Data Protection Policy

Executive Summary

The General Data Protection Regulation "Data Protection Law" sets out the principles that should be followed when dealing with information about individuals. This Policy reflects these data protection principles and regulates the use of such information.

Introduction

It is important that individuals read this Policy to ensure they are aware of the nature of the information that the School holds about individuals and reasons why the School needs to process this information, and to ensure they understand their responsibilities when dealing with information about others. Any breach of this policy will be taken seriously and may result in disciplinary action.

This policy must be complied with not only by staff and pupils, but also by individuals working in the School in other capacities, such as consultants, contractors, etc.

The policy impacts on a variety of people and the types of information that the School may be required to handle includes details of (not an exhaustive list):

- Current, past and future pupils;
- Parents of these pupils;
- Individual contacts of Suppliers;
- Individual contacts of Customers;
- Individual contacts at Local authorities and other agencies or government departments;
- Current, past and prospective staff;
- Individual donors; and
- Other individuals that we communicate with.

The personal information, which may be held on paper or on a computer or other media, is subject to certain legal safeguards specified in the UK GDPR and Data Protection Act 2018. The UK GDPR and Data Protection Act 2018 imposes restrictions on how the School may use the personal information.

This Policy is provided by way of guidance only and does not form part of an individual's contract with the School. The School may issue further guidance or amendments to this Policy from time to time and / or in line with legal developments or policy change.

Please note that the UK formally left the European Union on 1 January 2021 the UK that Eastbourne College (Eastbourne College Incorporated) will operate as Data Controller within UK domestic law via the UK Data Protection Act 2018 (the UK DPA). Further information on the UK DPA and UK Data Protection governance can be obtained online at https://ico.org.uk.

Statement of the School's Duties

The School shall process relevant personal data regarding staff and pupils and their parents and / or guardians as part of its operation and may process other personal data as listed above. The School shall

process such personal data in accordance with this Policy. "Processing" includes obtaining, handling, storage, transportation, recording, holding, disclosing, destroying or otherwise using personal data.

The Eastbournian Society (and its constituents) also processes data on behalf of Eastbourne College Incorporated (registered charity 307071) including, without limitation, for the following purposes:

- inviting members to social and other events
- putting members in contact with other Eastbournian Society members
- sharing contacts for career opportunities
- contacting them for fund-raising opportunities and donations
- contacting members for contributions to Eastbournian Society publications
- accessing databases to canvass for donations and inviting individuals to fundraising events
- publishing names of donors in Eastbournian Society publications

The School and any person or staff member who processes personal data on behalf of the School or for the School on behalf of the Eastbournian Society shall:

- Only process personal data fairly and lawfully;
- Only process for limited purposes and in an appropriate way, always specify one or more purposes when collecting personal data then only use that data for those purposes;
- Only collect personal data that is adequate, relevant and not excessive for the purposes specified;
- Keep personal data accurate and up-to-date;
- Keep personal data only as long as is necessary for the purpose;
- Process personal data in accordance with the rights of the people who are the subject of the data.

Keep the personal data secure and adopt technical and organisation measures to prevent:

- Unauthorised or unlawful processing of personal data;
- Against accidental loss or destruction of, or damage to, personal data;
- Not transfer personal data to people or organisations situated in countries without adequate protection.

Privacy Officer

The Schools have appointed Joseph Burge as Privacy Officer who will deal with all your requests and enquiries concerning the school's uses of your personal data, and endeavour to ensure that all personal data is processed in compliance with this policy and Data Protection Law. Joseph may be contacted by post, telephone or email using the details below.

Eastbourne College, Old Wish Road, Eastbourne, East Sussex, BN21 4JY

+44 (0) 1323 452300

jcburge@eastbourne-college.co.uk.

Whilst the Privacy Officer has overall responsibility for ensuring compliance, it is important to note that it is the responsibility of every member of staff / consultant / contractor who processes personal data on behalf of the School or for the School on behalf of the Eastbournian Society to comply with the UK GDPR and Data Protection Act 2018 and this Policy. Given the nature of the personal data which is being

processed, the School would like to stress the importance of compliance by every member of staff / consultant / contractor.

Personal Data

Personal data covers both facts and opinions about an individual. It includes any information which relates to or can identify an individual. It relates to data held on computers or held manually in files. The School may process a wide range of personal data of pupils, their parents or guardians, staff and others, as part of its operation. This personal data may include (but is not limited to): names and addresses; email addresses; telephone numbers; bank details; donations; academic, discipline, admissions and attendance records; references; photographs; examination scripts and marks; and general employee information.

Processing of Personal Data

The day to day working of the School necessarily involves the processing of personal data. The School also needs to collect and use personal data about individuals for a variety of personnel, and pupil administration and School management purposes. These purposes include payment of salary and operation of the payroll system, collection of fees, the provision and administration of staff and pupils, carrying out appraisals, performance reviews, salary reviews and promotion assessments, etc. It is also required to fulfil our contractual regard to the Parents' Contract and other legal obligations.

The UK GDPR and Data Protection Act 2018 seeks to ensure that the processing of personal data is done fairly and without adversely affecting the rights of the individuals who are the subject of the data. The individuals who the School processes personal information about must be told who the data controller is (in this case Eastbourne College Incorporated or the Eastbournian Society), who the data controller's representative is (in this case the Data Protection Officer), the purpose for which the data is to be processed by the School, and the identities of anyone to whom the data may be disclosed or transferred. This information will generally be provided in the Parents' Contract documentation for personal data of pupils and parents collected on the admission of a pupil and will be provided to staff in their employment contracts and related documentation.

However, staff / consultants / contractors need to bear these points of principle in mind for the processing of other personal data or for the provision of new personal data in relation to pupils / parents and staff or where changes to the use of the personal data or to whom it is needed to be disclosed to changes from when it was first collected by the School.

Any information which falls under the definition of personal data, and is not otherwise exempt, will remain confidential and will only be disclosed to third parties with the consent of the appropriate individual or other terms of this Policy.

Sensitive Personal Data

The School may, from time to time, be required to process sensitive personal data regarding an individual. Sensitive personal data includes medical information and data relating to religion, race, or criminal records and proceedings. Where sensitive personal data is processed by the School, the explicit consent of the appropriate individual will generally be required in writing.

The School holds information relating to individuals' health such as records of sickness absence and medical certificates (including the School's self-certified Sickness Form and any doctor's certificates). The School

may ask an individual to complete a medical questionnaire or undertake a medical examination and will therefore hold and use the resulting medical report. One of the purposes of finding out and keeping this sort of information is to administer and pay benefits related to ill-health such as the School and statutory sick pay, private medical insurance, long term disability schemes and life assurance. This information is needed to monitor and manage sickness absence and to ensure compliance with our obligations under the Disability Discrimination Act 1995 and health and safety legislation.

To enable the School to monitor the effectiveness of its Equal Opportunities Policy, individuals may be asked to complete a form, which contains sensitive personal data relating to ethnic origin, age, gender, etc. The responses are analysed on an anonymous basis and are not used for any other purpose.

The School may also record details of union membership (for purposes of deducting fees from salary and for collective consultation), CRB specific information and criminal records.

CCTV

Another form of personal data that the School holds is images recorded on the various CCTV cameras. All CCTV cameras are clearly labelled and are in place for the purpose of crime detection, for the security and welfare of staff and pupils and the protection of our working environment. Images are usually kept for no longer than is necessary to meet this purpose. Further details can be found in the School's CCTV policy document.

Storage of Personal Data

Personnel Files

Most of the types of employee information described above are kept in our personnel files. These files are located in the HR Department and access to the files is limited to staff in the HR Department. The HR Department will only allow other staff to view or copy information in the personnel file if it is essential for them to carry out their duties of employment.

Pupil Files

Parents' and pupils' information is also held by data managers in the Headmaster's Office. Prospective parents' and pupils' data is administered by the Registrar.

Some personal data described above may be kept in managers', individual teachers' or Heads of Departments' own filing system either in addition to, or instead of, being kept in the main personnel files. It is a manager, teacher or Head of Department's duty to ensure that any personal information is held securely, and that this data protection policy is complied with.

Some personal data of present and past pupils, parents and donors may also be kept in paper filing systems held by the Eastbournian Society or the School Archive. In addition, such personal data may be held in the Eastbournian Society's computer database for its processing of such data on behalf of the School, the Society and its constituents.

Computer Databases and Management Information Systems

Some or all of the sorts of personal information described above may be kept on a database, in order to facilitate the more efficient keeping and processing of the information.

Access to any such database is limited, and the School puts in place security measures to ensure the confidentiality of the information held on these systems. All security measures are regularly reviewed in line with legal and / or technological developments.

Other Means of Storage

Personal data is also held in other means of storage such as contact details in business cards, mobile telephones, diaries and paper filing systems.

Accurate and Up-to-Date Information

The School takes steps to keep the personal data it holds accurate and up-to-date. Employees must ensure they inform the relevant data manager if there are any changes to personal details. Managers must also ensure that any personal data held about others is accurate and only stored for as long as is necessary.

Personnel files, pupil and parent records and other personal data relating to staff, pupils and other individuals are kept for a reasonable time after they have left the School employment or have stopped dealing with the School. The School needs to do this in order to ensure benefits have been properly administered, to give references if requested to do so, to ensure that the School's tax and regulatory obligations have been satisfied and to deal with any tribunal or other court proceedings. The School will also retain personal information sufficient for fundraising and other charitable purposes. These records may be archived and stored by an external service provider.

The school reviews the period it holds personal data which is consistent with the principles laid out in the UK GDPR and Data Protection Act 2018.

Transferring Personal Data to Others

General Position

The School may make some personal data available to others such as lawyers, accountants, to those providing products or services to the School (such as ICT and other outsourcing providers) and to government and / or regulatory authorities.

Data Protection Rights

The UK GDPR and Data Protection Act 2018 gives staff, pupils and any other individuals about whom personal data is held, specific rights in relation to the information that is held about them. Under the UK GDPR and Data Protection Act 2018, a member of staff, pupil, parent (and individuals outside the School) are able to:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling.

A staff member or other individual may ask to see the personal data the School holds by requesting this in writing to the Privacy Officer. The School will respond to such requests as soon as it is practicable.

There should be awareness that certain data is exempt from the rights of access under the UK GDPR and Data Protection Act 2018. This may include information which identifies other individuals, information which the School reasonably believes is likely to cause damage or distress, or information which is subject to legal professional privilege. The School is also not required to disclose any pupil examination scripts.

The School will also treat as confidential any reference given by the School for the purpose of the education, training or employment, or prospective education, training or employment. The School acknowledges that an individual may have the right to access a reference relating to them received by the School. However, such a reference will only be disclosed if such disclosure will not identify the source of the reference or where, notwithstanding this, the referee has given their consent or if disclosure is reasonable in all the circumstances.

Responsibilities

As well as having rights under the UK GDPR and Data Protection Act 2018, all employees, pupils and parents need to comply with the data protection rules set out in this Policy and, in particular, in this section.

Personal Information

In order to assist the School in ensuring that personal information is kept up to date, it is a member of staff's responsibility to inform the HR Department and / or other relevant department of any changes.

Other People's Personal Information

It may be part of an individual's job to hold personal data about staff, pupils or other individuals, or there may be times when requests are made to supply personal data. Therefore, all employees need to take steps to ensure that they follow the guidelines set out below. Failure to follow the guidelines may result in disciplinary action, or in the case of serious misuse, referral to the Information Commissioner or the police.

Please note that the following guidelines apply equally to documents containing personal information which are kept in files as well as information which is kept in a computer database.

- All personal information must be kept securely and should remain confidential.
- Care must be taken about the personal information that is kept to ensure that real reasons exist for keeping it and to ensure that information is not kept longer than necessary.
- Any request from someone outside the School for personal data about an individual, which is not part of the normal running of the School, should be referred to the HR Department (employee) or Headmaster's office (parent or pupil). The School needs to verify the identity of the person making such a request and has to balance various considerations when deciding whether and how to respond to such a request, including compliance with the UK GDPR and Data Protection Act 2018.
- It is a criminal offence under the UK GDPR and Data Protection Act 2018 to deliberately or recklessly disclose personal data of an individual to someone outside the School without the School's and the individual's consent.
- Accessing, disclosing or otherwise using staff or employee records or other personal data without authority will be treated seriously and may result in disciplinary action being taken.

- If required to send personal data to a third party, avoid sending personal data which is confidential by email or by fax unless the link is secure and confidential. Also first ensure that the School has the appropriate authority to send the personal data to a third party eg with the consent of the appropriate individual or in accordance with terms of this Policy. Where there is any uncertainty as to whether the School has the appropriate authority, please check with the PRIVACY OFFICER.
- The School should not keep personal data about staff, pupils or individuals which is no longer needed, or which is out of date or inaccurate. Therefore, a regular review of any personal information held should take place, bearing these principles in mind.

Any uncertainty about the application of these guidelines regarding information held should be clarified through the PRIVACY OFFICER.

Use of Personal Information by the School

With consent, the School will, from time to time, make use of personal data relating to staff, pupils, their parents or guardians in the following ways. Any individual wishing to withdraw consent should notify the PRIVACY OFFICER in writing.

- To make use of photographic images in School publications and on the School website. However, the School will not publish photographs of individual pupils with their names on the School website.
- For fundraising, marketing or promotional purposes and to maintain relationships with pupils and parents of the School, including transferring information to any association, society or club set up for the purpose of establishing or maintaining contact with pupils or for fundraising, marketing or promotional purposes. As an example, personal data is transferred by the School to the Eastbournian Society for the purposes outlined above.

Security

The School will take reasonable steps to ensure that members of staff will only have access to personal data relating to staff, pupils, their parents or guardians or others where it is necessary for them to do so. All staff / consultants / contractors will be made aware of this policy and their duties under the UK GDPR and Data Protection Act 2018. The School will ensure that all personal information is held securely and is not accessible to unauthorised persons.

Security procedures include:-

- Entry controls. Any stranger seen in entry-controlled areas should be reported.
- Secure lockable desks and cupboards. Desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential).
- Methods of disposal. Paper documents should be shredded. Floppy disks, digital storage devices, CD-ROMs etc should be physically destroyed when they are no longer required.
- Equipment. Data users should ensure that individual monitors do not show confidential information to passers-by and that they lock their PC's when it is left unattended. Passwords for PC's should not be shared or transferred to other members of staff.
- Any personal data stored digitally must be encrypted or password protected.

Privacy notices are included in Appendix I of this policy.

Providing Information over the Telephone

Any member of staff dealing with telephone enquiries should be careful about disclosing any personal information held by the School. In particular they should:

- Check the caller's identity to make sure that information is only given to a person who is entitled to it. Where necessary, take the required details of the caller and ring back, this includes calls from outside agencies, eg Children's Services, the police.
- Suggest that the caller put their request in writing if they are not sure about the caller's identity and where their identity cannot be checked.
- Refer to the PRIVACY OFFICER for assistance in difficult situations. No-one should be bullied into disclosing personal information.

Enforcement

If an individual believes that the School has not complied with this Policy or acted otherwise than in accordance with the UK GDPR and Data Protection Act 2018, they should utilise the School complaints procedure and should also notify the PRIVACY OFFICER.

Date of this policy:	April 2021
Policy drawn up by:	JMG & JCB
Date of next policy review:	April 2022
Date for publication of revised policy:	May 2022
Submitted to governors:	Summer term 2019

Appendix I

Privacy Notice (Pupils)

UK GDPR and Data Protection Act 2018: How we use Pupil Information

We collect and hold personal information relating to our pupils and may also receive information about them from their previous school, local authority and / or the Department for Education (DfE). We use this personal data to:

- support our pupils' learning
- monitor and report on their progress
- provide appropriate pastoral care; and
- assess the quality of our services

This information will include their contact details, national curriculum assessment results, attendance information, any exclusion information, where they go after they leave us and personal characteristics such as their ethnic group, any special educational needs they may have as well as relevant medical information. For pupils enrolling for post 14 qualifications, the Learning Records Service will give us the unique learner number (ULN) and may also give us details about your learning or qualifications.

Over the age of 13, the law requires us to pass on certain information to the Local Authority who have responsibilities in relation to the education or training of 13-19 year olds. We may also share certain personal data relating to children aged 16 and over with post-16 education and training providers in order to secure appropriate services for them. A parent / guardian can request that only their child's name, address and date of birth be passed to other agencies by informing the College. This right is transferred to the child once he / she reaches the age 16.

We will not give information about our pupils to anyone without prior consent unless the law and our policies allow us to do so. If you want to receive a copy of the information about your son / daughter that we hold, please contact:

- Philippa Briggs hmsec@eastbourne-college.co.uk

We are required, by law, to pass some information about our pupils to the Department for Education (DfE). This information will, in turn, then be made available for use by the LA.

DfE may also share pupil level personal data that we supply to them, with third parties. This will only take place where legislation allows it to do so and it is in compliance with the Data Protection Act 1998.

Decisions on whether DfE releases this personal data to third parties are subject to a robust approval process and are based on a detailed assessment of who is requesting the data, the purpose for which it is required, the level and sensitivity of data requested and the arrangements in place to store and handle the data. To be granted access to pupil level data, requestors must comply with strict terms and conditions covering the confidentiality and handling of data, security arrangements and retention and use of the data.

For more information on how this sharing process works, please visit:

https://www.gov.uk/guidance/national-pupil-database-apply-for-a-data-extract

For information on which third party organisations (and for which project) pupil level data has been provided to, please visit:

https://www.gov.uk/government/publications/national-pupil-database-requests-received

If you need more information about how our local authority and / or DfE collect and use your information, please visit the DfE website at

https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

Privacy Notice (Staff and Others Working in the School)

UK GDPR and Data Protection Act 2018: How we use your Information

We process personal data relating to those we employ to work at, or otherwise engage to work at the College. This is for employment purposes to assist in the running of the school and / or to enable individuals to be paid. The collection of this information will benefit both national and local users by:

- improving the management of workforce data across the sector
- enabling development of a comprehensive picture of the workforce and how it is deployed
- informing the development of recruitment and retention policies
- allowing better financial modelling and planning
- enabling ethnicity and disability monitoring; and
- supporting the work of the School Teachers' Review Body

This personal data includes identifiers such as names and National Insurance numbers and characteristics such as ethnic group, employment contracts and remuneration details, qualifications and absence information.

We will not share information about you with third parties without your consent unless the law allows us to. We are required, by law, to pass on some of this personal data to:

- our local authority
- the Department for Education (DfE)

If you require more information about how we and / or DfE store and use your personal data please visit:

- https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

If you want to see a copy of information about you that we hold, please contact:

- Lee Swallow hr@eastbourne-college.co.uk

Appendix 2

Data Protection Basics

What is data protection?

Data protection is the fair and proper use of information about people. It's part of the fundamental right to privacy – but on a more practical level, it's really about building trust between people and organisations. It's about treating people fairly and openly, recognising their right to have control over their own identity and their interactions with others, and striking a balance with the wider interests of society.

What is 'personal data'?

In short, personal data means information about a particular living individual. This might be anyone, including a parent, pupil, employee, partner, member, supporter, business contact, public official or member of the public.

It doesn't need to be 'private' information – even information which is public knowledge or is about someone's professional life can be personal data.

It doesn't cover truly anonymous information – but if you could still identify someone from the details, or by combining it with other information, it will still count as personal data.

It only includes paper records if you plan to put them on a computer (or other digital device) or file them in an organised way such as a planner (A bucket of post-it notes is not personal data). For public authorities, all paper records are technically included – but they will be exempt from most of the usual data protection rules for unfiled papers and notes.

What is 'processing'?

Almost anything you do with data counts as processing; including collecting, recording, storing, using, analysing, combining, disclosing or deleting it.

Processing MUST have a legal reason for doing so. These are covered by the attached LAWFUL BASIS FOR PROCESSING QUICK REFERENCE word document.

What is a 'data subject'?

This is the technical term for the individual whom particular personal data is about.

With the above in mind, when processing personal data we should always consider if that personal data relates to a data subject.

Does the data 'relate to' an identifiable data subject?

It will often be clear where data 'relates to' a particular individual. However, sometimes this is not so clear and it may be helpful to consider in more detail what 'relates to' means.

Data which identifies an individual, even without a name associated with it, may be personal data if you are processing it to learn or record something about that individual, or where the processing has an impact on that individual.

Example

If data about a job salary is included in a vacancy advertisement, it will not, in those circumstances, be personal data. However, if the same salary details are linked to a name (for example, when the vacancy has been filled and there is a single named individual in post), the salary information about the job is personal data 'relating to' that employee.

Does the purpose of the processing make information personal data?

If the data is used, or is likely to be used, to learn, evaluate, treat in a certain way, make a decision about, or influence the status or behaviour of an individual, then it is personal data.

Is data that refers to an identifiable individual, but does not relate to them, personal data?

Data can contain references to an identifiable individual, or be linked to them, but not 'relate to' them as it is not about that individual but is about another topic entirely. Depending on the circumstances, this data may or may not be personal data.

Example

Emails written by a teacher to parents about their child will contain references to the teacher in the email signature - place of work, telephone number and email address which is personal data belonging to the teacher. However, the content of the email is not about (does not relate to) the teacher, but the pupil. The content of the email is not, therefore, personal data about the teacher or parent.

Do you have a particular scenario you have faced that you would like guidance on? Please email Joseph Burge JCBurge@eastbourne-college.co.uk

Some sample questions are:

Q: We have engaged a tutor or coach who does not work for the college, is it ok to email them pupil information?
A: Yes but with some caveats. The email of the tutor or coach must not be shared with another third party such as a family member and the data shared should be the minimum required for them to perform their service.

Q: We have sent all parents of children applying for a scholarship an email to provide them with scheduling information. If the parents are BCCd is it ok to include first names, surname initial and times of all children applying in the email body?
A: While parent identity is protected by the use of BCC, personal data that relates to the pupils would be shared with all parents. The impact to pupils may be low, but splitting the communication so that each parent is sent data relating to their child only would be preferred.

Q: Can we display pupil photographs and allergy information on posters around the school?
A: Personal medical data is protected to a greater degree than other types but our duty of care trumps data protection as long as the posters are only where needed and only for as long as needed.

Q: Do we need consent to take photographs of current pupils for use in communication to current parents?
A: No, regular content-rich communication to parents can form part of our service offering. Unless used for marketing, no consent is required.

Q: Can ID card, sport team, house, class or year photographs with pupils names printed on be created if consent has not been granted to photograph that pupil?
A: ID Cards fall under legal obligation, specifically our obligation to protect pupils and keep them safe partially relies on being able to identify them.

For other group and team photographs, we have a solid case for Public Interest in that class photos are of great interest to pupils, their families and friends going back generations and are cherished memories of their time at the school. Having a name under a prize winner is certainly in the public interest but naming pupils in a brochure cover image is not appropriate.

While only one legal reason for processing is required, we also have a Business Interest in that for many parents and grandparents, it is expected that these photos and the validation and recognition they provide and it would harm our business to cease to provide them.

In general, most individuals who deal with us are not data protection experts and it is often simpler to adopt a belt and braces approach to avoid any instance where we must prove we are working in a trustworthy and compliant manner. Please do contact me with any queries you may have.

Appendix 3

Lawful basis for processing quick reference

Overview

When we process personal data, we must have a lawful reason for doing so. While the ICO maintain each lawful reason is equal, the current guidance from law firms is to use consent only if it is absolutely necessary because it can be withdrawn at any time and can have a significant administrative overhead. The order below is from the most simple to identify and implement to the most complex and hardest to implement and contains some headline bullet points from the ICO.

- You must have a valid lawful basis in order to process personal data.
- There are six available lawful bases for processing. No single basis is 'better' or more important than the others – which basis is most appropriate to use will depend on your purpose and relationship with the individual.
- Most lawful bases require that processing is 'necessary'. If you can reasonably achieve the same purpose without the processing, you won't have a lawful basis.
- You must determine your lawful basis before you begin processing, and you should document it. Take care to get it right first time - you should not swap to a different lawful basis at a later date without good reason.
- Your privacy notice should include your lawful basis for processing as well as the purposes of the processing.
- If your purposes change, you may be able to continue processing under the original lawful basis if your new purpose is compatible with your initial purpose (unless your original lawful basis was consent).
- If you are processing special category data you need to identify both a lawful basis for general processing and an additional condition for processing this type of data.
- If you are processing criminal conviction data or data about offences you need to identify both a lawful basis for general processing and an additional condition for processing this type of data.

Vital Interests

It's clear from Recital 46 that vital interests are intended to cover only interests that are essential for someone's life. So, this lawful basis is very limited in its scope, and generally only applies to matters of life and death.

- You are likely to be able to rely on vital interests as your lawful basis if you need to process the personal data to protect someone's life.
- The processing must be necessary. If you can reasonably protect the person's vital interests in another less intrusive way, this basis will not apply.
- You cannot rely on vital interests for health data or other special category data if the individual is capable of giving consent, even if they refuse their consent.
- You should consider whether you are likely to rely on this basis, and if so document the circumstances where it will be relevant and ensure you can justify your reasoning.

Legal Obligation

In short, when you are obliged to process the personal data to comply with the law.

Article 6(3) requires that the legal obligation must be laid down by UK or EU law. Recital 41 confirms that this does not have to be an explicit statutory obligation, as long as the application of the law is foreseeable to those individuals subject to it. So it includes clear common law obligations.

This does not mean that there must be a legal obligation specifically requiring the specific processing activity. The point is that your overall purpose must be to comply with a legal obligation which has a sufficiently clear basis in either common law or statute.

You should be able to identify the obligation in question, either by reference to the specific legal provision or else by pointing to an appropriate source of advice or guidance that sets it out clearly. For example, you can refer to a government website or to industry guidance that explains generally applicable legal obligations.

- You can rely on this lawful basis if you need to process the personal data to comply with a common law or statutory obligation.
- This does not apply to contractual obligations.
- The processing must be necessary. If you can reasonably comply without processing the personal data, this basis does not apply.
- You should document your decision to rely on this lawful basis and ensure that you can justify your reasoning.
- You should be able to either identify the specific legal provision or an appropriate source of advice or guidance that clearly sets out your obligation.

Contract

The processing must be necessary to deliver your side of the contract with this particular person. If the processing is only necessary to maintain your business model more generally, this lawful basis will not apply and you should consider another lawful basis, such as legitimate interests.

This does not mean that processing which is not necessary for the contract is automatically unlawful, but rather that you need to look for a different lawful basis.

You have a lawful basis for processing if you have a contract with the individual and you need to process their personal data to comply with your obligations under the contract or you haven't yet got a contract with the individual, but they have asked you to do something as a first step (e.g. provide a quote) and you need to process their personal data to do what they ask.

It does not apply if you need to process one person's details but the contract is with someone else or if you take pre-contractual steps on your own initiative or at the request of a third party.

- You can rely on this lawful basis if you need to process someone's personal data:
- to fulfil your contractual obligations to them; or
- because they have asked you to do something before entering into a contract (eg provide a quote).
- The processing must be necessary. If you could reasonably do what they want without processing their personal data, this basis will not apply.
- You should document your decision to rely on this lawful basis and ensure that you can justify your reasoning.

Legitimate Interests

Legitimate interests is the most flexible lawful basis, but you cannot assume it will always be appropriate for all of your processing.

If you choose to rely on legitimate interests, you take on extra responsibility for ensuring people's rights and interests are fully considered and protected.

Legitimate interests is most likely to be an appropriate basis where you use data in ways that people would reasonably expect and that have a minimal privacy impact. Where there is an impact on individuals, it may still apply if you can show there is an even more compelling benefit to the processing and the impact is justified.

You can rely on legitimate interests for marketing activities if you can show that how you use people's data is proportionate, has a minimal privacy impact, and people would not be surprised or likely to object – but only if you don't need consent under PECR. See our Guide to PECR for more on when you need consent for electronic marketing.

Article 6(1)(f) gives you a lawful basis for processing where:

"processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child."

This can be broken down into a three-part test:

1. Purpose test: are you pursuing a legitimate interest?
2. Necessity test: is the processing necessary for that purpose?
3. Balancing test: do the individual's interests override the legitimate interest?

A wide range of interests may be legitimate interests. They can be your own interests or the interests of third parties, and commercial interests as well as wider societal benefits. They may be compelling or trivial, but trivial interests may be more easily overridden in the balancing test.

The UK GDPR specifically mentions use of client or employee data, marketing, fraud prevention, intra-group transfers, or IT security as potential legitimate interests, but this is not an exhaustive list. It also says that you have a legitimate interest in disclosing information about possible criminal acts or security threats to the authorities.

You must balance your interests against the individual's interests. In particular, if they would not reasonably expect you to use data in that way, or it would cause them unwarranted harm, their interests are likely to override yours. However, your interests do not always have to align with the individual's interests. If there is a conflict, your interests can still prevail as long as there is a clear justification for the impact on the individual.

- Legitimate interests is the most flexible lawful basis for processing, but you cannot assume it will always be the most appropriate.
- It is likely to be most appropriate where you use people's data in ways they would reasonably expect and which have a minimal privacy impact, or where there is a compelling justification for the processing.
- If you choose to rely on legitimate interests, you are taking on extra responsibility for considering and protecting people's rights and interests.
- Public authorities can only rely on legitimate interests if they are processing for a legitimate reason other than performing their tasks as a public authority.

- There are three elements to the legitimate interests basis. It helps to think of this as a three-part test. You need to:
  - identify a legitimate interest;
  - show that the processing is necessary to achieve it; and
  - balance it against the individual's interests, rights and freedoms.
- The legitimate interests can be your own interests or the interests of third parties. They can include commercial interests, individual interests or broader societal benefits.
- The processing must be necessary. If you can reasonably achieve the same result in another less intrusive way, legitimate interests will not apply.
- You must balance your interests against the individual's. If they would not reasonably expect the processing, or if it would cause unjustified harm, their interests are likely to override your legitimate interests.
- Keep a record of your legitimate interests assessment (LIA) to help you demonstrate compliance if required.
- You must include details of your legitimate interests in your privacy information.

Public Task

Any organisation who is exercising official authority or carrying out a specific task in the public interest. The focus is on the nature of the function, not the nature of the organisation.

Article 6(1)(e) gives you a lawful basis for processing where:

"processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller"

This can apply if you are either carrying out a specific task in the public interest which is laid down by law or exercising official authority (for example, a public body's tasks, functions, duties or powers) which is laid down by law.

If you can show you are exercising official authority, including use of discretionary powers, there is no additional public interest test. However, you must be able to demonstrate that the processing is 'necessary' for that purpose.

- You can rely on this lawful basis if you need to process personal data:
- 'in the exercise of official authority'. This covers public functions and powers that are set out in law; or
- to perform a specific task in the public interest that is set out in law.
- It is most relevant to public authorities, but it can apply to any organisation that exercises official authority or carries out tasks in the public interest.
- You do not need a specific statutory power to process personal data, but your underlying task, function or power must have a clear basis in law.
- The processing must be necessary. If you could reasonably perform your tasks or exercise your powers in a less intrusive way, this lawful basis does not apply.
- Document your decision to rely on this basis to help you demonstrate compliance if required. You should be able to specify the relevant task, function or power, and identify its statutory or common law basis.

Consent

Consent is one lawful basis for processing, but there are alternatives. Consent is not inherently better or more important than these alternatives. If consent is difficult, you should consider using an alternative.

Consent is appropriate if you can offer people real choice and control over how you use their data and want to build their trust and engagement. But if you cannot offer a genuine choice, consent is not appropriate. If you would still process the personal data without consent, asking for consent is misleading and inherently unfair.

If you make consent a precondition of a service, it is unlikely to be the most appropriate lawful basis.

Public authorities, employers and other organisations in a position of power over individuals should avoid relying on consent unless they are confident they can demonstrate it is freely given.

- The UK GDPR sets a high standard for consent. But you often won't need consent. If consent is difficult, look for a different lawful basis.
- Consent means offering individuals real choice and control. Genuine consent should put individuals in charge, build trust and engagement, and enhance your reputation.
- Check your consent practices and your existing consents. Refresh your consents if they don't meet the UK GDPR standard.
- Consent requires a positive opt-in. Don't use pre-ticked boxes or any other method of default consent.
- Explicit consent requires a very clear and specific statement of consent.
- Keep your consent requests separate from other terms and conditions.
- Be specific and 'granular' so that you get separate consent for separate things. Vague or blanket consent is not enough.
- Be clear and concise.
- Name any third-party controllers who will rely on the consent.
- Make it easy for people to withdraw consent and tell them how.
- Keep evidence of consent – who, when, how, and what you told people.
- Keep consent under review and refresh it if anything changes.
- Avoid making consent to processing a precondition of a service.
- Public authorities and employers will need to take extra care to show that consent is freely given and should avoid over-reliance on consent.