



Cefnogi Trydydd
Sector **Cymru**

Third Sector
Support **Wales**

GDPR Toolkit

This guidance is to be used by the recipient only and should not be passed to third parties without our consent.

UK GDPR compliance: checklist for third sector organisations

UK GDPR compliance: checklist for third sector organisations

Area of UK GDPR activity	Description of UK GDPR requirement	Actions	Status
Governance	One of the underlying principles of the UK GDPR is to ensure that organisations place data governance at the heart of what they do. As a result, the UK GDPR introduces a number of requirements to ensure that compliance is a serious focus for companies.	<ul style="list-style-type: none"> Documented a privacy governance model, for example, with clear roles and responsibilities and reporting lines to embed privacy compliance into the organisation, and address situations where there may be conflicting objectives internally Appoint a statutory data protection officer (https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/guide-to-accountability-and-governance/data-protection-officers/) (DPO) (if required or appropriate) or other person with responsibility for managing data protection compliance. Review insurance coverage and consider whether it needs to be updated in the light of the higher fines and penalties under the UK GDPR. Implement a data protection policy, which brings together all underlying related policies including processes for privacy by design and the creation and maintenance of a record of processing activities Integrate privacy compliance into your existing audit framework. 	
Training	Within the organisation, it is important to raise awareness of privacy issues and embed privacy compliance so that the organisation is proactive not reactive.	<ul style="list-style-type: none"> Develop and roll-out training across all personnel to ensure understanding of data protection principles, responsibilities and risks. Note – staff involved in activities such as marketing, computer security or data management may need specialist training to educate them on the data protection requirements for their particular area of work. Examples of training and guidelines for staff would include ensuring staff understand, among other things: <ul style="list-style-type: none"> The organisation's duties under the UK GDPR and the restrictions on the use of personal data. How to keep personal data secure. The correct process for deletion of data that may include personal data. How to keep back-ups of information. To take care when opening emails and attachments. To prevent cyber attacks. To comply with data subject requests. Record attendance at training events. 	

Area of UK GDPR activity	Description of UK GDPR requirement	Actions	Status
Accountability	One of the threads that runs through the UK UK GDPR is the requirement for organisations to have documentation to be able to demonstrate how they comply with the UK GDPR.	<ul style="list-style-type: none"> Review your existing grounds for lawful processing and confirm that these are still sufficient under the UK GDPR and ensure that the lawful basis for processing is explained in your processing records (see below). Consider whether your organisation is processing any special categories of personal data or criminal convictions data and ensure the requirements for processing such data are satisfied. 	
Consent	<p>The UK GDPR imposes requirements relating to valid consent: consent must be freely given, specific, informed and unambiguous. There must be positive opt-in (consent cannot be inferred from silence), consent must be separate from other terms and conditions and simple options to withdraw consent must be available.</p> <p>Consider whether the specific requirements relating to consent from children apply to your organisation (see "Children").</p>	<ul style="list-style-type: none"> Where consent is relied upon as the ground for processing personal data, review existing consents to ensure they meet the UK GDPR requirements, and if not implement a process to seek new consents. Ensure systems can record consent so that the organisation can demonstrate it has obtained consent. Keep a record of: <ul style="list-style-type: none"> Who consented: individual name or username. When consent was obtained: date and timestamp. How consent was obtained: a copy of the signed privacy statement or, for oral consents, a note of the conversation. For online requests, the information submitted together with a timestamp to link it back to the correct version of the data capture form should be kept. What was consented to: details of exactly what was consented to, on a granular level. Information provided to the individual: a copy of the privacy policy or notice provided to the individual which satisfies the various notification requirements of the UK GDPR. Ensure systems can accommodate withdrawal of consent and keep accurate records of data in respect of consent withdrawal and the activities ceased as a result of such withdrawal. Note - it may be possible to retain data and process it for a different purpose under another lawful basis, but the individual should have been made aware of such potential re-use of their data at the time of collection of data. 	
Legitimate Interests	"Legitimate interests" is one of the lawful bases which you can rely on to process personal data. If you are relying on it, you must be clear about the legitimate interests and ensure that they are not overridden by the privacy rights of the data subjects.	<ul style="list-style-type: none"> Identify where you are relying on legitimate interests to process data and undertake legitimate interests assessment to establish whether the processing is lawful. Ensure that privacy notices explain the legitimate purposes and include the right to object in a prominent place. 	

Area of UK GDPR activity	Description of UK GDPR requirement	Actions	Status
Privacy Notices	There is a greater emphasis on transparency in the UK GDPR. Notices must be clear, concise and informative. Data subjects must be adequately informed of all data processing activities and data transfers and the information set out in Articles 13 to 14 of the UK GDPR must be provided. This includes the legal basis for the processing of personal data.	<ul style="list-style-type: none"> Review and update privacy notices to ensure that they are UK GDPR compliant. Consider adopting a comprehensive privacy notice with shorter specific privacy notices on relevant forms and on-line as required. 	
Children	The UK GDPR requires parental consent for certain types of processing of children's personal data, but it is best practise to do this for all types of data processing. The UK has determined the relevant age at which a child can give their own consent is 13.	<ul style="list-style-type: none"> If data relating to a child will be processed, ensure that age-verification systems are in place, notices directed at that child are "child-friendly" and, if consent is relied upon, you have implemented a mechanism to seek parental consent Consider alternative protections, for example, age-gating which is the term used for automated ways of only enabling access to on-line systems for people above a certain age. 	
HR	Employees must be adequately informed of all data processing activities and data transfers. It is inappropriate to rely on consent for processing employee data	<ul style="list-style-type: none"> Review and update employee and candidate notices to be UK GDPR compliant. Identify the lawful basis of processing of employee data. Update contracts of employment to remove employee consents for processing of personal data (if applicable). 	

Area of UK GDPR activity	Description of UK GDPR requirement	Actions	Status
Data subject rights and procedures	<p>The UK GDPR grants data subjects the right to:</p> <ul style="list-style-type: none"> • Receive certain information about the controller's personal data collection and processing activities. • Access their personal data. • Correct their personal data. • Erase personal data, also known as the right, to be forgotten. • Restrict personal data processing. • Receive a copy of certain personal data or transfer personal data to another controller, also known as the data portability, right. • Object to personal data processing. • Not be subject to automated decision-making under certain circumstances. <p>Receive notifications of security breaches.</p>	<ul style="list-style-type: none"> • Update data privacy policy and internal processes for dealing with requests. • Ensure technical and operational processes are in place to ensure data subjects' rights can be met, for example, right to be forgotten, data portability, the right to object and subject access requests. • Ensure staff members are able to recognise data subjects' rights requests and then process such requests efficiently, given the one-month timeframe in the legislation for responding to such requests. 	
Records of processing	<p>The UK GDPR requires organisations to maintain a detailed record of all processing activities, including purposes of processing, a description of categories of data, security measures and comprehensive data flow map. A number of stakeholders will need to be involved in creating and maintaining this data record.</p>	<ul style="list-style-type: none"> • Identify all data processed in a detailed record of processing. For example, document what personal data is held by your organisation, where it came from and who it is shared with, the legal basis for processing and the security measures in place (or DPIAs). • Implement and maintain processes for updating and maintaining records of processing. 	
Data transfers outside the UK	<p>The UK GDPR only permits export of personal data outside the UK if certain conditions apply. The penalties for breaching these restrictions range from significant fines to a block on the transfer of data itself.</p> <p>The general rule is that transfers of personal data outside the UK are only permitted with no further safeguards where the destination jurisdiction is deemed to offer an adequate level of protection for the data. In the absence of adequacy regulations, an organisation may still make a transfer subject to appropriate safeguards, including:</p> <ul style="list-style-type: none"> • Binding corporate rules. • ICO approval standard contractual clauses. • The ICO's own International Data Transfer Agreement. • An ICO approved code of conduct or certification mechanism. 	<ul style="list-style-type: none"> • Identify whether you are using any systems hosted outside the UK. • Identify if you transfer data outside the UK. • Identify the basis on which you are doing it to ensure the transfer is lawful • Ensure the above is included in your privacy notice. 	

Area of UK GDPR activity	Description of UK GDPR requirement	Actions	Status
Security	Data controllers must ensure appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.	Ensure appropriate security has been implemented, including backups, encryption and regular testing to ensure technical security (see the ICO information security checklist - https://ico.org.uk/for-organisations/advice-for-small-organisations/getting-started-with-gdpr/data-protection-self-assessment-medium-busineses/)	
Data breach procedures	The UK GDPR stipulates mandatory reporting of personal data breaches that are likely to result in a risk to the rights and freedoms of individuals. The process requires organisations to act quickly, mitigate losses and, where mandatory notification thresholds are met, notify regulators (within 72 hours) and affected data subjects (if merited, without undue delay).	<ul style="list-style-type: none"> Review and update (or develop where not in existence) a data breach response plan. Review insurance coverage for data breaches and consider whether it needs to be updated in the light of the higher fines and penalties under the UK GDPR. Review provisions in agreements dealing with breaches caused by service providers and other partners. Consider in advance what other obligations may be owed, including to other regulators, in the event of a data breach and the triggers for notification applied in the context of the business operations. 	
Sharing Data	<p>The UK GDPR changes the liability regime for data processors, making them directly liable for compliance. It also increases the controls on appointing a data processor.</p> <p>It is essential to identify all organisations with which you share personal data and work out the basis of the relationship and whether you have a controller / processor relationship or a joint controller relationship.</p>	<ul style="list-style-type: none"> Identify third parties with whom your organisation shares personal data and establish if they are data processors acting on your behalf or joint controllers. Carefully document the steps you have taken when appointing data processors to ensure that they will keep data secure. Enter into updated data sharing agreements with partner organisations. Enter into UK GDPR compliant data processing agreements with all data processors including considering whether you wish to impose any particular security measures on the data processors. Establish security protocols for transferring personal data with third parties. 	

Area of UK GDPR activity	Description of UK GDPR requirement	Actions	Status
Retention	Data controllers are required not to keep personal data in an identifiable form for any longer than is necessary for the purposes for which personal data is processed.	<ul style="list-style-type: none"> Establish a retention policy for all personal data that the organisation holds. Reference this in your privacy notice. 	
Privacy by design and default	<p>In keeping with the UK GDPR's objective to bring privacy considerations to the forefront of organisation decision making, the UK GDPR requires data protection requirements to be considered when new technologies are designed or on-boarded or new projects using data are being considered.</p> <p>Data protection impact assessments (DPIAs) should be used to ensure compliance in any event, but these will be mandatory for projects where data processing is likely to result in a high risk to individuals.</p> <p>A DPIA must contain:</p> <ul style="list-style-type: none"> A systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable the legitimate interest pursued by the controller. An assessment of the necessity and proportionality of the processing operations in relation to the purposes. An assessment of the risks to the rights and freedoms of data subjects. The measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with the UK GDPR taking into account the rights and legitimate interests of data subjects and other persons concerned. <p>Where a DPIA indicates that the processing presents a high risk in the absence of measures taken by the controller to mitigate the risk, controllers are required to consult the ICO before commencing processing.</p>	<ul style="list-style-type: none"> Ensure processes are in place to embed privacy by design into projects (for example, technical and organisational measures are in place to ensure data minimisation, purpose limitation and security) Put in place a data protection impact assessment (DPIA) protocol and carry out DPIAs and keep records of the same. Consult with the ICO when appropriate. 	

The Lawful Bases for Processing Personal Data under the UK General Data Protection Regulation (UK GDPR): Guidance Note

This short guidance note is to help you identify the potential relevant legal bases for your Privacy Notice. It does not constitute legal advice and may not be relied on for that purpose. Your organisation should take separate legal advice on the content of any Privacy Notice before it is finalised

The Lawful Bases for Processing Personal Data under the UK General Data Protection Regulation (UK GDPR) – Guidance Note

The UK GDPR sets high standards for the protection of personal data and imposes a number of obligations on those handling the data.

Under the UK GDPR, organisations must have a valid lawful basis in order to process personal data. There are six available lawful bases for processing ordinary personal data under Article 6 of the UK GDPR:

1. Consent.
2. Necessary in connection with a contract.
3. Necessary to comply with legal obligation.
4. To protect vital interests.
5. Public interest or official authority.
6. Legitimate interests.

The ICO has produced a [Lawful basis interactive guidance tool](#) which is intended to help organisations decide the lawful basis that they can use.

Lawful Basis	Explanation
The data subject has given consent to the processing of their personal data for one or more specific purposes	<p>Consent is one lawful basis for processing, but there are alternatives. Consent is not inherently better or more important than these alternatives and in fact, there may be occasions where it is not appropriate.</p> <p>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. It presents the individual with a false choice and only the illusion of control. You must identify therefore the most appropriate lawful basis for processing from the start.</p> <p>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.</p> <p>If you are relying on consent, you need to document the consent. Consent must be freely given, specific, informed and unambiguous. There must be positive opt-in (consent cannot be inferred from silence), consent must be separate from other terms and conditions and simple options to withdraw consent must be available without detriment.</p>

Lawful Basis	Explanation
	<p>You must ensure separate consent is obtained for each purpose for which you process personal data.</p> <p>Consent is currently an essential requirement when sending unsolicited marketing communications to individuals by electronic methods under regulations closely associated with the UK GDPR, called the Privacy and Electronic Communications Regulations. The standard for consent is the UK GDPR standard. The ICO adopts a very broad definition of marketing communications, and this is likely to include sending newsletters to your supporters as well as messages publicising your events and making fundraising asks.</p>
Processing is necessary for entering or performing a contract with the data subject	<p>You have a lawful basis for processing if:</p> <ul style="list-style-type: none"> • Your organisation has a contract with the individual and you need to process their personal data to comply with your obligations under the contract. • Your organisation hasn't yet got a contract with the individual, but you need to process their personal data in order to enter into a contract. <p>This basis does not apply if you need to process one person's details, but the contract is with someone else.</p> <p>In this context, a contract does not have to be a formal signed document, or even written down, as long as there is an agreement which meets the requirements of contract law. The processing must be necessary to deliver your side of the contract with the particular person.</p> <p>A common example of where this applies is in the case of employees or people who are applying to work for you. This gives an employer scope to rely on performance of a contract where the processing of data is necessary and can be linked back to the contract. Examples where this category would be appropriate in the employment context include providing:</p> <ul style="list-style-type: none"> • Home address details for communications. • Bank details to pay salary under the contract. • Next of kin for life assurance and other relevant benefits.
Processing is necessary for compliance with a legal obligation to which the data controller is subject	<p>This applies when you are obliged to process the personal data to comply with the law.</p> <p>This can be any legal obligation, including common law. Your overall purpose must be to comply with a legal obligation which has a sufficiently clear basis in either common law or statute.</p> <p>Good examples of this include where you need to comply with health and safety legislation, your obligation to provide information to the Charity Commission and to HMRC.</p>

Lawful Basis	Explanation
Processing is necessary to protect the vital interests of the data subject	<p>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.</p> <p>This ground is likely to be particularly relevant for emergency medical care, when it is necessary to process personal data for medical purposes, but the individual is incapable of giving consent to the processing. However, data concerning health is special category personal data and is subject to the grounds for processing set out in Article 9 of the UK GDPR.</p>
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	<p>Although this lawful basis will usually only apply to public bodies any organisation which carries a task out in the public interest can rely on it. The task must, however, be laid down by the law so there is overlap between this and the legal obligation basis.</p>
Processing is necessary for the purposes of legitimate interests pursued by the data controller, except where these interests are overridden by the interests for the fundamental rights and freedoms of the data subject which require the protection of personal data (in particular where the data subject is a child).	<p>"Legitimate interests" is the most flexible lawful basis for processing, but you cannot assume it will always be the most appropriate.</p> <p>It is likely to be most appropriate where your organisation is using 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.</p> <p>There are three elements to the legitimate interests basis. The ICO recommends that you think of this as a three-part test.</p> <p>You need to:</p> <ul style="list-style-type: none"> • identify a legitimate interest; • show that the processing is necessary to achieve it; and • balance it against the individual's interests, rights and freedoms. <p>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.</p> <p>The processing must be necessary. If you can reasonably achieve the same result in another less intrusive way, legitimate interests will not apply.</p> <p>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.</p> <p>You should keep a record of the legitimate interests assessment undertaken by your organisation.</p> <p>You must include details of your legitimate interests in your privacy notice. Where processing is based on this lawful basis, the data subject must be given the right to object, which should be highlighted in the privacy notice.</p>

No single basis is 'better' or more important than the others – which basis is most appropriate to use will depend on your organisation's purpose and relationship with the individual.

Most lawful bases require that processing is 'necessary'. If your organisation can reasonably achieve the same purpose without the processing, your organisation won't have a lawful basis. Your organisation must determine the lawful basis before it begins processing, and this should be documented. You should take care to get it right first time – your organisation should not swap to a different lawful basis at a later date without good reason.

Your organisation's privacy notice should include your lawful basis for processing as well as the purposes of the processing. There may be categories of data to which more than one ground for processing potentially applies. Where data is being processed for more than one reason, all the grounds should be listed so it is transparent to an employee what is being done with their data.

The advantage to you of stating more than one ground is that if one falls away, there is still another basis for processing.

Special categories of personal data

If your organisation is processing special category data, you will need to identify both a lawful basis under Article 6 of the UK GDPR and a special category ground for processing under Article 9 of the UK GDPR. There are ten grounds on which special category data can be processed under Article 9 of the UK GDPR:

- 1. Explicit consent.** Where the data subject has given explicit consent for the processing of the personal data for one or more specified purposes.
- 2. Employment law rights and obligations.** Where it is necessary for carrying out rights and obligations under employment law.
- 3. Protection of vital interests.** Where it is necessary to protect the vital interests of the data subject or another person, where the data subject is physically or legally incapable of giving consent.
- 4. Foundations, associations or other not-for-profit bodies.** Where it is carried out with appropriate safeguards in the course of the legitimate activities of a foundation, association or other not-for-profit body which has a political, philosophical, religious or trade union aim. The processing must only relate to members or former members of that body, or persons who have regular contact with it, in connection with its purposes. Personal data must not be disclosed to anyone outside that body without the data subject's consent.
- 5. Made public by the data subject.** Where it relates to personal data which has been manifestly made public by the data subject.

- 6. Legal claims.** Where processing is necessary for the establishment, exercise or defence of legal claims, or whenever courts are acting in their judicial capacity.
- 7. Substantial public interest.** Where processing is necessary for reasons of substantial public interest.
- 8. Health purposes.** Where processing is necessary 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.
- 9. Public health.** Where processing is necessary 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.
- 10. Archiving, research and statistics.** Where processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) (as supplemented by section 19 of the DPA 2018) based on domestic law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

Five of the above grounds are subject to restrictions which require the processing to be authorised or based in law (as set out in section 10 and section 11 of the [Data Protection Act 2018](#) (DPA 2018) and any subordinate legislation made under it.

Criminal convictions and offences data

The UK GDPR provides additional safeguards in connection with the processing of personal data relating to criminal convictions and offences or personal data linked to related security measures.

Organisations must have a lawful basis under Article 6 of the UK GDPR and either legal authority under domestic law or official authority for the processing.

If you do not have official authority for the processing, it must be authorised by domestic law. In the UK, this authorisation in law is set out in the conditions listed in Schedule 1 of the DPA 2018.

Schedule 1 sets out 28 potential conditions for processing criminal offence data.

Schedule 1 (at paragraphs 5 and 38 to 41) also includes additional requirements for you to keep an appropriate policy document and records of processing in relation to criminal offence data. These requirements apply for some, but not all, of the conditions.

A data protection impact assessment may be required for any type of processing which is likely to be high risk.

GDPR – Privacy Notice Guidance Note

Sample GDPR – Privacy Notice

Guidance Note

This guidance note accompanies the Sample GDPR Privacy Notice template and is designed to provide drafting assistance for those implementing the policy. It outlines key considerations, best practices, and practical advice to ensure the policy is effectively and consistently applied. This tool aims to support clear and accurate policy drafting, helping to align with the organisation's objectives and legal requirements.

- **This guidance is to be used by the recipient only and should not be passed to third parties without our consent.**
- **Using this template - this template contains square brackets and highlighting to show the areas you will need to insert information and/or consider whether the options shown are relevant for your organisation. Your review should not be limited to these areas, as there may be areas in the template that are not relevant to your organisation and should be deleted.**
- **When you have finalised your notice, you should remove all the square brackets and highlighting.**
- **There is a short guidance note to help you identify the potential relevant legal bases. It does not constitute legal advice and may not be relied on for that purpose. Your organisation should take separate legal advice on the content of any Privacy Notice before it is finalised.**

Clause	Guidance
General	This has been drafted as a separate policy to one that would be used internally to notify employees/workers about the use of their personal data by their employer organisation.
Note 1	If it is likely that such special category data will be collected, then an enhanced privacy policy ought to be produced which sets out when this happens and the additional lawful bases justifying the processing.
Note 2	Transparency is key when dealing with children, as children do not lose their data subject rights just because consent has been given by a holder of parental responsibility. For this reason, privacy notices should be written in a concise, clear and plain style and as far as possible, be addressed directly to the relevant age group. If the target audience covers a wide age range or is aimed at parents, then different versions of the notice should be provided or, if only one is provided, it needs to be understood by the youngest age range.
Note 3	This will only be a relevant legal basis if the organisation has a clear basis in law for the underlying task, function or power.
Note 4	It is likely to be in rare circumstances that this legal basis is relied on but is included for completeness.



Introduction

We treat privacy and confidentiality very seriously. We are a [describe nature of the organisation i.e. charity / social enterprise] with relationships with fundraisers, volunteers, supporters and service users so we use personal data on a day to day basis in order to fulfil our [missional / vision] to [describe goals of organisation briefly]. Our use of personal data allows us to make better decisions, fundraise more efficiently and, ultimately, helps us to achieve our vision. We have developed this privacy notice in order to be as transparent as possible about the personal data we collect and use.

We comply with all aspects of the UK's data protection legislative framework, which includes the European General Data Protection Regulation (GDPR) and the UK's own legislation, including the Data Protection Act 2018.

Please ensure you read this notice carefully and contact us if you have any questions or concerns about our privacy practices.

Who we are?

In this Privacy Policy, “we” “us” or “our” means [Name of organisation] (registered charity in England and Wales (.....), a company limited by guarantee in England and Wales (.....) and our group company [] Trading Limited (company number in England and Wales).

We are the controller and responsible for your personal data.

We have appointed a dedicated [Data Protection Officer (DPO) / Data Privacy Manager] to ensure appropriate oversight of our data processing activities and who is responsible for overseeing questions in relation to this privacy notice. The [DPO/ Data Privacy Manager], is [] who can be contacted by telephone on [xxx] or by email [xxx] and can provide any clarity that you may need about this privacy notice, including any requests to exercise your legal rights.

What this Notice Covers?

We ask that you read this privacy notice carefully as it contains important information about:

- how we collect your personal data
- the types of personal data that we collect and use
- the lawful bases we rely on to collect and use personal data
- why we collect and use personal data
- sharing your personal data
- when we transfer personal data outside of the UK
- how long we keep personal data
- how we ensure personal data is secure; and
- your privacy rights

You should ensure that you read this general privacy notice alongside any specific privacy notice we may issue to you, from time to time, in relation to your information.

How we collect your personal data

We collect data in the following ways:

- You may give us your personal data in order [to complete a contact form, to sign up for one of our events, sign up for a newsletter, make a donation, purchase our products, register as a volunteer for us, join our [] network, apply for funding, use our services] or otherwise communicate with us.
- When you use our website, we collect your personal data using “cookies” and other similar tracking methods and technologies. [There are more details on the cookies and tracking methods we use in our Cookie Policy].

- In addition, in accordance with common website practice, we will receive information about the type of device you're using to access our website or apps and the settings on that device may provide us with information about your device, including what type of device it is, what specific device you have, what operating system you're using, what your device settings are, and why a crash has happened. Your device manufacturer or operating system provider will usually have more details about what information your device makes available to us.

If you wish to give us personal data about another person, please speak to us to ensure that you are legally entitled to give us the information and for advice on informing that person.

Your information may be shared with us by third parties, for example:

- professional fundraising agencies;
- independent event organisers, for example the London Marathon or fundraising sites like Just Giving or Virgin Money Giving;
- if you sign up as a volunteer for us through an external volunteering website;
- if your information is shared with us by []

[We also may receive data about you from suppliers acting on our behalf who provide us with technical, payment or delivery services, and from business partners, advertising networks and search/analytics providers used on our website.]

Social Media

Depending on your settings or the privacy policies for social media and messaging services like Facebook, WhatsApp or Twitter, you might give us permission to access information from these services, for example when you publicly tag us in an event photo.

Information available publicly

We may supplement information on our supporters with information from publicly available sources such as charity websites and annual reviews, corporate websites, public social media accounts, the electoral register and Companies House in order to create a fuller understanding of your reason for supporting us. For more information, please see our section on "Building profiles of supporters" below.

The types of personal data that we collect and use

Personal data means any information about an individual from which the person can be identified.

The data that we may collect, use, store and transfer includes different kinds of personal data about you as follows:

- your name
- your contact details (including postal address, telephone number, e-mail address and/or social media identity)
- your date of birth
- your gender
- your bank or credit card details where you provide these to make a payment
- if you volunteer for us or apply for a job with us, information necessary for us to process these applications and assess your suitability (which may include things like employment status, previous experience depending on the context, as well as any unspent criminal convictions or pending court cases you may have)
- if you apply for funding, information necessary to process your application, such as [give details]
- information about your activities on our website(s) and about the device you use to access these, for instance your IP address and geographical location
- information about events, activities and products which you have shown an interest in
- information relating to your health (for example if you are taking part in or attending an event for health and safety purposes,
- information you may choose to share with us about your experience of [include details] where you have left us a legacy, any information regarding next of kin with which you may have provided us to administer this
- information as to whether you are a taxpayer to enable us to claim Gift Aid
- age, sexual orientation, disability and nationality and ethnicity information for monitoring purposes;
- marketing and communications data which includes your preferences in receiving marketing from us and our third parties and your communication preferences; and
- any other personal data you provide to us].

Certain types of personal data are in a special category under data protection laws, as they are considered to be more sensitive. Examples of this type of data include information about health, race, religious beliefs, political views, trade union membership, sex life or sexuality and genetic/biometric information.

We only collect this type of information about you to the extent that there is a clear reason for us to do so or where you make it public or volunteer it to us. Wherever it is practical for us to do so, we will make why we are collecting this type of information clear and what it will be used for. **[SEE GUIDANCE NOTE (1). PLEASE DELETE THIS COMMENT ONCE REVIEWED]**

The Personal Data of Children and Vulnerable Adults **[SEE GUIDANCE NOTE (2.) PLEASE DELETE THIS COMMENT ONCE REVIEWED]**

We are very careful when we collect personal data about children under the age of 13 and vulnerable adults.

Where we are collecting personal data about children under the age of 13, we provide a privacy notice to their parents or guardians for approval, and where necessary consent.

If you have any concerns please raise these with our [\[DPO / Data Privacy Manager\]](#).

The lawful bases that we rely on to collect and use personal data

We rely on the following legal bases to process your personal data *delete as appropriate*: When we use special category personal data (please see the “What personal data we collect” section above), we require an additional legal basis to do so under data protection laws, so will either do so on the basis of your explicit consent or another route available to us at law for using this type of information (for example if you have made the information manifestly public, we need to process it for employment, social security or social protection law purposes, your vital interests, or, in some cases, if it is in the public interest for us to do so).

Performance of a contract	This applies where we need to collect and use your personal data in order to take steps to enter into a contract with you or to perform our obligations under a contract with you.
Legal obligation	This applies where we need to collect and use your personal data to comply with applicable laws and regulatory requirements. We will identify the relevant legal obligation when we rely on this legal basis.
Legitimate interests	We may collect and use your personal data where it is necessary to conduct our business and pursue our legitimate interests. We only do this where we are satisfied that your privacy rights are protected satisfactorily. We make sure we consider and balance any potential impact on you and your rights (both positive and negative) before we process your personal data for our legitimate interests. We do not use your personal data for activities where our interests are overridden by the impact on you (unless we have your consent or are otherwise permitted to by law).
Consent	We rely on consent only where we have obtained your active agreement to use your personal data for a specified purpose.
Public task [SEE GUIDANCE NOTE (3.) PLEASE DELETE THIS COMMENT ONCE REVIEWED]	Although we are not a public body, we do collect and use some personal data where this is necessary to perform tasks that are in the public interests.
Vital Interests [SEE GUIDANCE NOTE (4). PLEASE DELETE THIS COMMENT ONCE REVIEWED]	This only applies in the rare instance where we need to process personal data in order to protect someone's life.

NB You should provide detailed information on all the specific legal bases that apply to your data processing of ordinary and special category personal data in the table below. There are a number of specific provisions contained in Schedule 1 of the Data Protection Act 2018 that enable lawful processing of special category data.

Why we collect and use personal data

We collect and use personal data for the following purposes, relying on the specific lawful bases set out in the table below *delete or add to as appropriate*. We have also identified what our legitimate interests are where appropriate:

Why	Legal Bases
To provide you with the services, products or information you asked for.	Consent Contract Legitimate interests
To administer your donation or support your fundraising, including processing Gift Aid.	Legitimate interests Legal obligation
To keep a record of your relationship with us.	Legitimate interests Legal obligation
To respond to or fulfil any requests, complaints or queries you make to us.	Legitimate interests Legal obligation
To better understand how we can improve our services, products or information by conducting analysis and market research.	Legitimate interests
To manage our events.	Contract Legitimate interests Legal obligation
To send you correspondence and communicate with you, including updating your contact details (see "Keeping your information up to date" below).	[Consent] Legitimate interests
To undertake analysis and profiling of our supporters using personal data we already hold.	Legitimate interests

Why	Legal Bases
To administer our websites and to troubleshoot, perform data analysis, research, generate statistics and surveys related to our technical systems.	Legitimate interests
To generate reports on our work, services and events.	Legitimate interests Legal obligation
To safeguard our staff and volunteers.	Legal obligation
To monitor website use to identify visitor location, guard against disruptive use, monitor website traffic and/or personalise information which is presented to you.	Consent Legitimate interests
To process your application for a job or volunteering position.	Contract Legitimate interests
To audit and administer our accounts.	Legal obligation
To meet our legal obligations to regulators, government and/or law enforcement bodies.	Legal obligation Legitimate interests
To undertake background checks including checking identity and checks undertaken for anti-money laundering, anti-terrorism reasons, financial and reputational checks. We do not undertake any automated decision making, but we use credit reference and fraud prevention agencies who may do so.	Legal obligation Legitimate interests
To train and develop our staff and volunteers.	Contract Legal obligation Legitimate interests
To prevent and respond to actual or potential fraud or illegal activities.	Legal obligation
To establish, exercise or defend our legal rights or for the purpose of legal proceedings in which we may be involved.	Legal obligation Legitimate interests

Sending marketing communications

Our marketing communications include information about our work, campaigns and requests for donations or other support. [Occasionally, we may include information from partner organisations or organisations who support us in these communications.]

[We operate an 'opt-in only' communication policy [for electronic communications]. This means that, except as set out below, we will only send electronic marketing communications to those that have explicitly stated that they are happy for us to do so.]

[We may use information you have given us directly, for example the record of your previous donations to and/or relationship with us, your location and demographics, as well as the type of activity you have been involved with, to tailor our communications with you about future activities.]

Events and fundraising

When you have asked for details of one of our events, we will send you information including, where relevant, ideas for fundraising and reminders on key information about the activity.

Where you have signed up for an event with a third party (for example the London Marathon) and told the event organiser that you wish to fundraise for us, we may contact you with information and support for your fundraising for that event.

Managing your contact preferences

We make it easy for you to tell us how you want us to communicate, in a way that suits you.

Our forms have clear marketing preference questions and we include information on how to opt out when we send you marketing. If you don't want to hear from us, that's fine, and you can change your preferences at any time. Just let us know when you provide your data or contact us [explain how for example] [by logging into the website and checking or unchecking relevant boxes to adjust your marketing preferences OR by following the opt-out links within any marketing communication sent to you or by contacting us [LINK]. If you've decided you don't want to be contacted for marketing purposes, we may still need to contact you for administrative purposes. This may include where we are processing a donation you've made and any related Gift Aid, thanking you for a donation or participation in an event, or keeping in touch with you about volunteering activities you are doing for us.

Building profiles of supporters

Our work is only made possible thanks to the generosity of our supporters – so it's vital that our fundraising efforts are as effective as they can be. By developing a better understanding of our supporters through researching them using publicly available sources, we can tailor and target our fundraising events and communications (including

volunteering opportunities) to those most likely to be interested in them. This allows us to be more efficient and cost-effective with our resources, and also reduces the risk of someone receiving information that they might find irrelevant, intrusive or even distressing.

After taking a supporter's communications preferences into account, we use information we hold on them to research their potential to make donations. We may collect additional details relating to their employment and any philanthropic activity. We may also estimate their gift capacity, based on their visible assets, history of charitable giving and how connected they are to us.

We use existing data from our own database and combine this with information from publicly available sources such as charity websites and annual reviews, corporate websites, public social media accounts, the electoral register and Companies House in order to create a fuller understanding of that supporter. We only use publically available reputable sources. We avoid any data that we believe has not been lawfully or ethically obtained. We're committed to putting you in control of your data and you're free at any time to opt out from this activity by taking the following action [INSERT.]

Sharing your personal data

A number of third parties may have access to your personal data or we may share or send it to them. This includes:

- business partners, suppliers and sub-contractors who may process information on our behalf;
- if you are a legacy giver, we may share information with co-beneficiaries;
- marketing agencies that we use
- analytics and search engine providers
- our professional advisers
- IT service providers.

We may also be required to share personal data with regulatory authorities, government agencies and law enforcement agencies. We will use reasonable endeavours to notify you before we do this, unless we are legally restricted from doing so.

We do not sell, rent or otherwise make personal data commercially available to any third party. We require all third parties to respect the security of your personal data and to treat it in accordance with the law. We do not allow our third-party service providers to use your personal data for their own purposes and only permit them to process your personal data for specified purposes and in accordance with our instructions.

We reserve the right to disclose your personal data to third parties:

- if we sell or buy any business or assets, in which case we may disclose your personal data to the prospective seller or buyer of such business or assets; and/or

- if substantially all of our assets are acquired by a third party, personal data held by us may be one of the transferred assets.

Transfers Outside the UK

We do not send personal data outside the UK. None of the service providers we use to help us run our businesses are based outside of the UK.

[it is very important to seek legal advice if this is not the case]

Keeping your information updated

We really appreciate it if you let us know if your contact details change, but to ensure that the data we have is as up to date and accurate as possible, we may use information from external sources such as the post office national change of address database and/or the public electoral roll to identify when we think you have changed address so that we can update our records and stay in touch. We only use sources where we are confident that you've been informed of how your information may be shared and used.

We do this so we can continue to contact you where you have chosen to receive marketing messages from us and contact you if we need to make you aware of changes to our terms or assist you with problems with donations.

This activity also prevents us from having duplicate records and out of date preferences, so that we don't contact you when you've asked us not to.

How long we keep personal data

Our policy is to not hold personal data for longer than is reasonably necessary to fulfil the purposes we collected it for. We may retain your personal data for a longer period in the event of a complaint or if we reasonably believe there is a prospect of litigation in respect of our relationship with you. We have established data retention timelines for all of the personal data that we hold based on why we need the information. The timelines take into account any statutory or regulatory obligations we have to keep the information, our ability to defend legal claims, our legitimate business interests, best practice and our current technical capabilities. We have developed a Data Retention Policy that captures this information. We delete or destroy personal data securely in accordance with the Data Retention Policy. A copy of these data retention guidelines is available from [INSERT].

How we ensure personal data is secure

We are strongly committed to information security and we take reasonable and appropriate steps to protect your personal data from unauthorised access, loss, misuse, alteration or corruption. We have put in place physical, electronic, and managerial procedures to safeguard and secure the information you provide to us including the use of encryption and pseudonymisation.

In addition, we limit access to your personal data to those employees, agents, contractors and other third parties who have a business need to know. They will only process your personal data on our instructions and they are subject to a duty of confidentiality.

We have put in place procedures to deal with any suspected personal data breach and will notify you and any applicable regulator of a breach where we are legally required to do so.

Your privacy rights

You have a number of rights in relation to your personal data which we have. Not all of the rights apply in all circumstances. If you wish to exercise any of the rights, please contact us in the ways detailed below:

- You have a right of access to the personal data we hold about you (commonly known as a “subject access request”). This enables you to receive a copy of the personal data we hold about you and to check that we are lawfully processing it.
- You have the right to ask us to correct any information we hold about you that you think is wrong or incomplete.
- You have the right to object to any processing of your personal data where we are relying on a legitimate interest (or those of a third party) as the legal basis to do so and you think that your rights and interests outweigh our own and you wish us to stop. There may, however, be legal or other legitimate reasons why we need to keep or use your information which override your right to object. If this is the case, we will consider your request and explain why we cannot comply with it. You can ask us to restrict the use of your personal data while we are considering your request.
- You have the absolute right to object if we process your personal data for the purposes of direct marketing. If you no longer want to receive communications from us, please contact us. We will stop sending you communications, but will continue to keep a record of you and your request not to hear from us. If we deleted all of your information from our direct marketing databases, we would have no record of the fact that you have asked us not to communicate with you and it is possible that you may start receiving communications from us at some point in the future, if we obtain your details from a different source.
- You have the right to request restriction of processing of your personal data. This enables you to ask us to suspend the processing of your personal data in one of the following scenarios:
 - o If you want us to establish the data's accuracy;
 - o Where our use of the data is unlawful but you do not want us to erase it;
 - o Where you need us to hold the data even if we no longer require it as you need it to establish, exercise or defend legal claims; or
 - o You have objected to our use of your data but we need to verify whether we have overriding legitimate grounds to use it.

- You have the right to ask us to delete your information. This is also known as the right to be forgotten or to erasure. We will not always agree to do this in every case as there may be legal or other legitimate reasons why we need to keep or use your information. If this is the case, we will consider your request and explain why we cannot comply with it. You can ask us to restrict the use of your personal data while we are considering your request.
- Where our processing of your personal data is based on your consent, you have the right to withdraw it at any time. Please contact us if you want to do so. Please note that this will not affect the lawfulness of any processing carried out before you withdrew your consent. If you withdraw your consent, we may not be able to provide certain products or services to you. We will advise you if this is the case at the time you withdraw your consent.

You may have a right to obtain the personal data that you have given us in a format that be easily re-used and to ask us to pass this personal data on in the same format to other organisations. Note that this right only applies to automated information which you initially provided consent for us to use or where we used the information to perform a contract with you. Please contact us to find out if this right applies to you.

If you wish to exercise any of the rights set out above, [please contact [INSERT]].

How to Complain

You have the right to make a complaint at any time to the Information Commissioner's Office (ICO), the UK regulator for data protection issues (www.ico.org.uk). We would, however, appreciate the chance to deal with your concerns before you approach the ICO so please contact us in the first instance.

You can contact us the following ways:

[add in the detail]

Changes to this Privacy Notice

This privacy notice was last updated on [] 2025. We keep this privacy notice under regular review and may change it from time to time by updating this page in order to reflect changes in the law and/or our privacy practices. We would encourage you to check this privacy notice for any changes on a regular basis.

GDPR Policy

"This guidance is to be used by the recipient only and should not be passed to third parties without our consent".

Sample policy on use of own devices by Trustees and Volunteers



Sample GDPR policy on use of own devices by Trustees and Volunteers



GDPR Policy

“This guidance is to be used by the recipient only and should not be passed to third parties without our consent”.

Sample policy on use of own devices by Trustees and Volunteers

- **Using this template – this template contains square brackets and highlighting to show the areas you will need to insert information and/or consider whether the options shown are relevant to your organisation.**
- **Your review should not be limited to these areas, as there may be areas in the template that are not relevant to your organisation and should be deleted.**
- **When you have finalised your policy, you should remove all the square brackets and highlighting.**
- **If you are unsure whether certain information applies to your organisation, you should take separate legal advice on the content of this policy before it is finalised.**

1. About this policy

- 1.1** [Name of Organisation] (the “Organisation,” “we”, or “us” or “ our”) recognises and acknowledges that our trustees and volunteers (referred to as you) are a very important and significant part of our workforce. Unfortunately, we cannot afford to provide all our trustees and volunteers with mobile telephones, tablets or laptops and therefore we have developed this policy to establish appropriate protocols for you to use your own devices to do work for the Organisation.
- 1.2** Allowing you to use your personal mobile devices for Organisation purposes gives rise to increased risk in terms of the security of our IT resources and communications systems, the protection of confidential and proprietary information and reputation, and compliance with legal obligations such as data protection requirements.
- 1.2.1** The purpose of this policy is to therefore set out our rules on the use of personal devices in order to:
 - 1.2.2** protect our systems and data;
 - 1.2.3** prevent our data from being deliberately or inadvertently lost, disclosed or altered;
 - 1.2.4** set out the circumstances in which we may monitor your use of our systems, access your device and retrieve, remove or destroy data on it and the action which we will take in respect of breaches of this policy.
- 1.3** Anyone covered by this policy may use an approved personal mobile device for Organisation purposes, provided that they sign the declaration at the end of this policy and adhere to its terms.
- 1.4** This policy supplements and should be read in conjunction with our other policies and procedures in force from time to time, including without limitation our [IT and communications systems policy OR IT acceptable use policy], [Privacy standard OR Data protection policy], [Data retention policy], and other IT related policies, which are available from [INSERT NAME].

2. Who is responsible for this policy?

- 2.1** The [board of directors (the Board) OR [COMMITTEE] OR [POSITION] has overall responsibility for the effective operation of this policy. The [Board OR [COMMITTEE] OR [POSITION]] has delegated responsibility for overseeing its implementation to [POSITION]. Questions about the content of this policy or suggestions for change should be reported to [POSITION].
- 2.2** Any questions you may have about the day-to-day application of this policy should be referred to [POSITION] in the first instance.
- 2.3** This policy is reviewed annually by [POSITION].

3. Scope and purpose of the policy

- 3.1** This policy applies to trustees and volunteers who use a personal mobile device including any accompanying software or hardware (referred to as a device in this policy) for organisation purposes. It applies to the use of the device both during and outside office hours and regardless of the location of use.

- 3.2** This policy applies to all devices used to access the organisation's IT resources and communications systems (collectively referred to as systems in this policy), which may include (but are not limited to) smartphones, mobile or cellular phones, tablets, and laptop or notebook computers.
- 3.3** When you access our systems you may be able to access data about [staff, other trustees, volunteers, service users, supporters, suppliers] and other contacts, including information which is confidential, proprietary or private and which may consist of personal data. The definition of data is very broad, and includes all written, spoken and electronic information held, used or transmitted by us or on our behalf, in whatever form (collectively referred to as Organisation Data in this policy).
- 3.4** When you access our systems using a device, we are exposed to a number of risks, including the loss or theft of the device (which could result in unauthorised access to our systems or Organisation Data), the threat of malware (such as viruses, worms, spyware, Trojans or other threats that could be introduced into our systems via a device) and the loss or unauthorised alteration of Organisation Data (including personal and confidential information which could expose us to the risk of non-compliance with legal obligations of confidentiality, data protection and privacy). Such risks could result in damage to our systems, our business and our reputation.
- 3.5** The purpose of this policy is to protect our systems and Organisation Data, and to prevent Organisation Data from being deliberately or inadvertently lost, disclosed or altered, while enabling you to access our systems using a device. This policy sets out the circumstances in which we may monitor your use of our systems, access your device and retrieve, remove or destroy data on it and the action which we will take in respect of breaches of this policy. More information about how we monitor, record and process personal data is contained in our separate [Privacy notice] and [Data protection policy].
- 3.6** Breach of this policy may lead to us revoking your access to our systems, whether through a device or otherwise. You are required to co-operate with any investigation into suspected breach, which may involve providing us with access to the device and any relevant passwords and login details.
- 3.7** Some devices may not have the capability to connect to our systems. We are not under any obligation to modify our systems or otherwise assist you in connecting to our systems.

4. Connecting devices to our systems

- 4.1** Connectivity of all devices is centrally managed by [the IT Department] who must approve a device before it can be connected to our systems. [Devices must comply with our [IT Security Policy].] [Devices must be on the approved list of devices, available from [POSITION] OR [the IT Department]]. You may apply for a device to be added to the approved list by submitting it to [POSITION] OR [the IT Department] who will have full discretion to approve or reject the device.

- 4.2** Before using your device to connect to our systems, or to access Organisation data, in accordance with this policy, you must:
- 4.2.1** register your device with [the IT Department]; and
 - 4.2.2** present your device to [the IT Department] for approval and configuration; and
 - 4.2.3** at our cost implement such technical security measures as [the IT Department] may reasonably require, including [insert details].
- 4.3** You are not permitted to use any device other than the device that has been registered and approved by us. We reserve the right to refuse or remove permission for your device to connect with our systems. [The IT Department] will refuse or revoke such permission (and may take all steps reasonably necessary to do so) where in our reasonable opinion a device is being or could be used in a way that puts, or could put, us, our staff, our contacts, our systems, or our Organisation Data at risk or that may otherwise breach this policy.
- 4.4** In order to access our systems it may be necessary for [the IT Department] to install software applications on your device. If you remove any such software, your access to our systems will be disabled.

5. Monitoring

- 5.1** The contents of our systems and Organisation Data are our property. All materials, data, communications and information, including but not limited to e-mail (both outgoing and incoming), telephone conversations and voicemail recordings, instant messages and internet and social media postings and activities, created on, transmitted to, received or printed from, or stored or recorded on a device (collectively referred to as content in this policy) during the course of the Organisation's operations or on our behalf is our property, regardless of who owns the device.
- 5.2** We reserve the right to monitor, intercept, review and erase, without further notice, all content on the device that has been created for us or on our behalf. This might include, without limitation, the monitoring, interception, accessing, recording, disclosing, inspecting, reviewing, retrieving and printing of transactions, messages, communications, postings, log-ins, recordings and other uses of the device as well as keystroke capturing and other network monitoring technologies, whether or not the device is in your possession.
- 5.3** It is possible that personal data on your device may be inadvertently monitored, intercepted, reviewed or erased. Therefore, you should have no expectation of privacy in any data on the device. You are advised not to use our systems for any matter intended to be kept private or confidential. If you use your device to process personal data about third parties (for example your family and friends) you should be aware that this may be inadvertently monitored, intercepted, reviewed or erased. You should ensure that any third parties are aware that their personal data may be inadvertently monitored.

- 5.4** Monitoring, intercepting, reviewing or erasing of content will only be carried out to the extent permitted by law in order for us to comply with a legal obligation or for our legitimate purposes, including, without limitation, in order to:
- 5.4.1** prevent misuse of the device and protect Organisation Data;
 - 5.4.2** ensure compliance with our rules, standards of conduct and policies in force from time to time (including this policy); and
 - 5.4.3** ensure that you do not use our facilities or systems for any unlawful purposes or activities that may damage our business or reputation.
- 5.5** We may also store copies of any content for a period of time after they are created and may delete such copies from time to time without notice. We may obtain and disclose copies of such content or of the entire device (including personal content) for litigation or investigations.
- 5.6** By signing the declaration at the end of this policy, you acknowledge that you have been made aware that the Organisation undertakes such monitoring where it has a legitimate basis to do so and you confirm your agreement (without further notice or permission) to our right to copy, erase or remotely wipe the entire device (including any personal data stored on the device). You also agree that you use the device at your own risk and that we will not be responsible for any losses, damages or liability arising out of its use, including any loss, corruption or misuse of any content or loss of access to or misuse of any device, its software or its functionality.
- 5.7** You must co-operate with us to enable such monitoring including providing any passwords or PIN numbers necessary to access the device or relevant applications.

6. Security requirements

[This list should be reviewed and tailored accordingly depending on the requirements of the organisation when it comes to personal devices and their use. Information that is not applicable should be removed. PLEASE DELETE THIS COMMENT ONCE CONSIDERED]

- 6.1** You must:
- 6.1.1** at all times, use your best efforts to physically secure the device against loss, theft or use by persons who we have not authorised to use the device. You must secure the device whether or not it is in use and whether or not it is being carried by you. This includes, but is not limited to, passwords, encryption, and physical control of the device;
 - 6.1.2** [install any anti-virus or anti-malware software at our request before connecting to our systems and consent to our efforts to manage the device and secure its data, including providing us with any necessary passwords];
 - 6.1.3** [comply with our device configuration requirements];

- 6.1.4 [protect the device with a PIN number or strong password, and keep that PIN number or password secure at all times. The PIN number or password should be changed every [NUMBER] weeks]. If the confidentiality of a PIN number or password is compromised, you must change it immediately. The use of PIN numbers and passwords should not create an expectation of privacy by you in the device;]
- 6.1.5 [not download and install software to the device unless explicitly authorised by us. A list of applications that are already authorised and those that are expressly forbidden is available from [POSITION]];
- 6.1.6 [not alter the security settings of the device without our consent];
- 6.1.7 [maintain the device's original operating system and keep it current with security patches and updates. Rooted (Android) or jailbroken (iOS) devices are strictly forbidden from accessing our systems or Organisation Data];
- 6.1.8 [ensure that anyone who may use your device from time to time, such as your family, friends and business associates do not have access to Organisation Data held on the device];
- 6.1.9 [not download or transfer any Organisation Data to the device, for example via email attachments, unless specifically authorised to do so. You must immediately erase any such information that is inadvertently downloaded to the device;]
- 6.1.10 [not backup the device locally or to cloud-based storage or services where that might result in the backup or storage of Organisation Data. Any such backups inadvertently created must be deleted immediately;]
- 6.1.11 [where we have permitted you to store Organisation Data on the device, ensure that the Organisation Data is encrypted using appropriate encryption technologies approved by [[POSITION] OR the IT Department];]
- 6.1.12 [not use the device as a mobile hot-spot without our prior consent.];
- 6.1.13 [not use public unsecured Wi-Fi to access our systems without our prior consent.];
- 6.1.14 [not sell, replace or transfer the device to anyone else without our prior consent].

7. Lost or stolen devices and unauthorised access

In the event of a lost or stolen device, or where you believe that a device may have been accessed by an unauthorised person or otherwise compromised, you must report the incident to [the IT Department] immediately.

Appropriate steps will be taken to ensure that Organisation Data on or accessible from the device is secured, including remote wiping of the device where appropriate. The remote wipe will destroy all Organisation Data on the device. Although we do not intend to wipe other data that is strictly personal in nature (such as photographs or personal files or emails), it may not be possible to distinguish all such information from Organisation Data in all circumstances. You should therefore regularly backup all personal data stored on the device.

8. Wiping devices

We reserve the right to remove your access to our systems and, where appropriate, remove any Organisation Data from the device, directly or remotely at any time. Although we do not intend to wipe any other data on your device it may not be possible to distinguish all such information from Organisation Data in all circumstances. You should therefore regularly backup any personal data contained on the device.

9. Technical support

We are unable to provide technical support for devices. If you use a device for charity purposes you are responsible for any repairs, maintenance or replacement costs and services.

10. Costs and Reimbursements

10.1 You must pay for your own device costs under this policy, including but not limited to voice and data usage charges and any purchase and repair costs. By signing the declaration at the end of this policy you acknowledge that you alone are responsible for all costs associated with the device and that you understand that your business usage of the device may increase your voice and data usage charges.

10.2 You also agree that you use the device at your own risk and that we will not be responsible for any losses, damages or liability arising out of its use, including any loss, corruption or misuse of any content or loss of access to or misuse of any device, its software or its functionality.

11. Changes to this policy

This policy notice was last updated on []. We keep this policy under regular review and may change it from time to time.

Declaration and Agreement

I wish to use my personal mobile device for [NAME OF ORGANISATION] purposes and explicitly confirm my understanding and agreement to the following:

- I have read, understood and agree to all of the terms contained in the Policy on the use of own devices by trustees and volunteers.
- I understand that the terms of this policy will apply to me at all times, during or outside office hours and at any location.
- I acknowledge and agree that authorised personnel of [NAME OF ORGANISATION] shall have the rights set out in this policy, including but not limited to the right to access, monitor, review, record and wipe (as the case may be) data contained on my personal device (which I acknowledge may result in inadvertent access to or destruction of my data).
- I understand and agree that [NAME OF ORGANISATION] in its discretion may amend, or remove this policy at any time and that I will be bound by the terms of the policy as amended.

.....
SIGNED

.....
PRINTED NAME

.....
DATE

Sample Data Protection Policy



Using these guidelines

- * Using this template – this template contains square brackets and highlighting to show the areas you will need to insert information and/or consider whether the options shown are relevant to your organisation. Your review should not be limited to these areas, as there may be areas in the template that are not relevant to your organisation and should be deleted.*
- * When you have finalised your policy, you should remove all the square brackets and highlighting.*
- * If you are unsure whether certain information applies to your organisation, you should take separate legal advice on the content of this policy before it is finalised.*

1. Introduction

This policy provides information about the data protection legislation, including the UK General Data Protection Regulation ("UK GDPR") and Data Protection Act 2018 with which [Organisation Name] ("the Organisation", "we", "our", "us") must comply.

This policy applies to all members of staff, trustees, volunteers and others who do work for us.

This policy provides a general overview of the legal requirements. It sets out what we expect from you in general terms when handling personal data, regardless of the format in which it is stored. This includes information about:

- Current or former employees and workers and applicants
- Current or former volunteers and applicants
- Current or former trustees and applicants
- [beneficiaries / clients / users of our services]
- Users of our on-line and digital media channels
- Current, former or potential supporters, donors and funders including individuals and representatives of organisations
- People with whom we engage in relation to our campaigning activity
- Representatives of organisations with whom we have partnerships, or we are collaborating
- Representatives of our suppliers

You must read, understand and comply with this policy when handling personal data on our behalf and attend any compulsory training on its requirements. The policy may be supplemented by specific guidance relevant to your role.

Your compliance with this policy is mandatory. Any breach of this policy may result in disciplinary action.

This policy is an internal document and cannot be shared with anyone outside the Organisation without prior authorisation from the [DPO/DPL].

2. Definitions

The following definitions are used in this policy:

Automated Decision-Making (ADM)

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

Automated Processing

Means 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, as are many uses of artificial intelligence (AI) where they involve the processing of Personal Data.

Consent

Means an 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.

Controller

Means the person or organisation that determines when, why and how to process Personal Data. We are the Data Controller of all Personal Data used in our organisation for our own purposes.

Criminal Convictions Data

Means personal data relating to criminal convictions and offences, including personal data relating to criminal allegations and proceedings.

Data Subject

Means 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)

Means a tools and assessment used to identify and reduce risks of a data processing activity. A DPIA can be carried out as part of Privacy by Design and should be conducted for all major system or business change programs involving the Processing of Personal Data.

[Data Protection Officer (DPO)] or [Data Protection Lead (DPL)]

Means the person with responsibility for data protection compliance within our organisation. The current person is [redacted].

Explicit Consent

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

UK GDPR

Means the retained EU law version of the General Data Protection Regulation ((EU) 2016/679) as defined in the Data Protection Act 2018. Personal Data is subject to the legal safeguards specified in the UK GDPR.

Personal Data

Means any information identifying a Data Subject or information relating to a Data Subject from which we can identify (directly or indirectly) a Data Subject whether from that data alone or in combination with other identifiers we possess or can reasonably access. Personal Data includes Special category 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

Means 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

Means implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the UK GDPR.

Privacy Notice or Privacy Policies

Means separate notices setting out information that may be provided to Data Subjects when we collect 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
- stand-alone, one-time privacy statements covering Processing related to a specific purpose.

Processing or Process

Means 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

means 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

means 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.

3. Data Protection Principles

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

- processed lawfully, fairly and in a transparent manner;
- collected only for specified, explicit and legitimate purposes;
- adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed;
- accurate and where necessary kept up to date;
- not kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the data is Processed;
- 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;
- not transferred to another country without appropriate safeguards in place; and
- made available to Data Subjects and allow Data Subjects to exercise certain rights in relation to their Personal Data.

We must also comply with particular legal requirements when suppliers that carry out services for us have access to Personal Data and when we are working with organisations and need to share Personal Data.

We are responsible for and must be able to demonstrate compliance with the requirements under the law.

4. Lawfulness, Fairness and Transparency

Personal data must be Processed lawfully, fairly and in a transparent manner in relation to the Data Subject.

You may only collect, Process and share Personal Data fairly and lawfully and for specified purposes. The law 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.

The lawful bases available when processing non-special category personal data are:

- the Data Subject has given consent to the processing of his or her personal data for one or more specific purposes
- the processing is necessary for the performance of a contract between us and the Data Subject or in order to take steps at the request of the Data Subject prior to entering into a contract
- the processing is necessary for compliance with a legal obligation to which we are subject
- the processing is necessary in order to protect the vital interests of the Data Subject or of another natural person
- the processing is necessary for the performance of a task carried out in the public interest
- the processing is necessary for the purposes of legitimate interests we are pursuing or which a third party is pursuing, 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.

A range of additional legal requirements apply when processing Special Category Personal Data or Criminal Convictions Data. These are set out in the Data Protection Act 2018. Please see the definitions section for the types of information this includes. If your role involves you being required to process Special Category Personal Data or Criminal Convictions Data, you will receive additional guidance on this.

5. Consent

[UK GDPR sets a high standard for consent which has in many cases required businesses to change their consent mechanisms. Relying on inappropriate consent could leave the organisation exposed to enforcement action. Organisations should keep records to evidence consent including who consented, when, how, and what they were told. Consent needs to be refreshed "at appropriate intervals" and the ICO recommends every two years as a rough guide- PLEASE DELETE ONCE CONSIDERED]

A Controller must only process Personal Data on one or more of the lawful bases set out in the UK GDPR, which include Consent.

A Data Subject consents to Processing of their Personal Data if they clearly indicate agreement to the Processing. Consent requires affirmative action, so silence, pre-ticked boxes or inactivity will not be sufficient to indicate consent. If Consent is given in a document which deals with other matters, then the Consent must be kept separate from those other matters.

A Data Subject must be easily able to withdraw Consent to Processing at any time and withdrawal must be promptly honoured. Consent may need to be refreshed if you intend to Process Personal Data for a different and incompatible purpose which was not disclosed when the Data Subject first consented.

When processing Special Category Data or Criminal Convictions Data, we will usually rely on a legal basis for processing other than Explicit Consent or Consent if possible. Where Explicit Consent is relied on, you must issue a Privacy Notice to the Data Subject to capture Explicit Consent.

You will need to evidence Consent captured and keep records of all Consents so that we can demonstrate compliance with Consent requirements.

6. Transparency

The law requires us to provide detailed, specific information about our use of Personal Data to Data Subjects. Such information must be provided through appropriate Privacy Notices which must be concise, transparent, intelligible, easily accessible, and in clear and plain language so that a Data Subject can easily understand them.

Whenever we collect Personal Data directly from Data Subjects, we must provide the Data Subject with information including who we are and how and why we will Process, disclose, protect and retain their Personal Data. This is done through a Privacy Notice which must be presented when the Data Subject first provides the Personal Data.

When Personal Data is collected indirectly (for example, from a third party or publicly available source), we must provide the Data Subject with the Privacy Notice information as soon as possible after collecting/receiving the data. We must also check that the Personal Data was collected by the third party in accordance with law and on a legal basis which contemplates our proposed Processing of that Personal Data.

If you are collecting Personal Data from a Data Subject, directly or indirectly, then you must provide the Data Subject with a Privacy Notice in accordance with this policy.

7. Purpose Limitation

Personal Data must be collected only for specified, explicit and legitimate purposes. It must not be further Processed in any manner incompatible with those purposes.

You cannot use Personal Data for new, different or incompatible purposes from that disclosed when it was first obtained unless you have informed the Data Subject of the new purposes and there is a legal basis for doing so.

If you want to use Personal Data for a new or different purpose from that for which it was obtained, you must first contact the [DPO/DPL] for advice on how to do this in compliance with both the law and this policy.

8. Data Minimisation

Personal Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed.

You may only collect Personal Data that you require for your duties: you should not collect excessive data. You should ensure any Personal Data collected is adequate and relevant for the intended purposes.

You must ensure that when Personal Data is no longer needed for specified purposes, it is deleted or anonymised in accordance with our applicable data retention guidelines.

9. Accuracy

Personal Data must be accurate and, where necessary, kept up to date. It must be corrected or deleted without delay when inaccurate.

You should 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. You should check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards. You must take all reasonable steps to amend inaccurate or out-of-date Personal Data.

10. Retention

Personal Data must not be kept in an identifiable form for longer than is necessary for the purposes for which the data is processed. We will maintain retention policies and procedures to ensure Personal Data is deleted securely in accordance with this requirement. You must comply with our retention policies.

11. Security integrity and confidentiality

Personal Data must be secured by appropriate technical and organisational measures against unauthorised or unlawful Processing, and against accidental loss, destruction or damage.

You are responsible for protecting the Personal Data we hold. You must ensure that you follow all guidelines issued to you that are designed to protect against unlawful or unauthorised Processing of Personal Data and against the accidental loss of, or damage to, Personal Data. You must exercise particular care to protecting Special Category Personal Data and Criminal Convictions Data from loss and unauthorised access, use or disclosure.

You must follow all procedures and technologies we put in place to maintain the security of all Personal Data from the point of collection to the point of destruction. You may only transfer Personal Data to third-party service providers who agree to comply with the required policies and procedures and who agree to put adequate measures in place, as requested.

You must maintain data security by protecting the confidentiality, integrity and availability of the Personal Data, defined as follows:

- Confidentiality: only people who have a need to know and are authorised to use the Personal Data can access it;
- Integrity: Personal Data is accurate and suitable for the purpose for which it is processed; and
- Availability: authorised users are able to access the Personal Data when they need it for authorised purposes.

You must comply with and not attempt to circumvent the administrative, physical and technical safeguards we implement and maintain in accordance with the UK GDPR and relevant standards to protect Personal Data.

You may only Process Personal Data when required to do so as part of your role. You cannot Process Personal Data for any reason unrelated to your role.

12. Reporting a Data Breach

The UK GDPR requires Data Controllers to notify any Personal Data Breach to the Information Commissioner's Office (ICO) and, in certain instances, the Data Subject. If you know or suspect that a Personal Data Breach has occurred, do not attempt to investigate the matter yourself. You should immediately contact the [DPO/DPL]. You should preserve all evidence relating to the potential Personal Data Breach and provide assurance to the [DPO/DPL] as required.

13. Transfer Limitation

The UK GDPR restricts data transfers to countries outside the UK to ensure that the level of data protection afforded to individuals by the UK GDPR is not undermined. You transfer Personal Data originating in one country across borders when you transmit, send, view or access that data in or to a different country.

You may only transfer Personal Data outside the UK if one of the following conditions applies:

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

If you need to send Personal Data outside the UK, you should contact the [DPO/DPL] immediately for advice.

14. Data Subject Rights

Data Subjects have rights when it comes to how we handle their Personal Data. These include rights to:

- where Processing is based on the legal basis of consent, to withdraw Consent to Processing at any time;
- receive certain information about our Processing activities;
- request access to their Personal Data that we hold (including receiving a copy of their Personal Data);
- prevent our use of their Personal Data for direct marketing purposes;
- ask us to erase Personal Data if it is no longer necessary in relation to the purposes for which it was collected or Processed or to rectify inaccurate data or to complete incomplete data;
- restrict Processing in specific circumstances;

- object to Processing which has been justified on the basis of our legitimate interests or in the public interest;
- request a copy of an agreement under which Personal Data is transferred outside of the UK;
- object to decisions based solely on Automated Processing, including profiling (ADM);
- prevent Processing that is likely to cause damage or distress to the Data Subject or anyone else;
- be notified of a Personal Data Breach which is likely to result in high risk to their rights and freedoms; and
- in limited circumstances, receive or ask for their Personal Data to be transferred to a third party in a structured, commonly used and machine readable format.

You must verify the identity of an individual requesting data under any of the rights listed above (do not allow third parties to persuade you into disclosing Personal Data without proper authorisation).

You must immediately forward any Data Subject request you receive to the [DPO/DPL].

15. Sharing Personal Data

You may only transfer Personal Data to third-party service providers who agree to comply with our policies and procedures and who agree to put adequate security measures in place, as requested. We must have a written contract in place with any such service providers we are using. This contract must contain specific information in line with UK GDPR requirements and you should liaise with the [DPO/DPL] on this.

In addition, although it is not a legal requirement, it is good practice to agree data sharing arrangements in writing with any partners with which we are working where the relationship involves sharing Personal Data. It is essential that you have a clear legal basis for sharing Personal Data with such partners or any third parties and that you transmit the Personal Data securely.

16. Accountability

The Controller must implement appropriate technical and organisational measures in an effective manner to ensure compliance with data protection principles. The Controller is responsible for, and must be able to demonstrate, compliance with the data protection principles.

We must have adequate resources and controls in place to ensure and to document UK GDPR compliance including:

- appointing a suitably qualified DPO (where necessary) or DPL responsible for data privacy;

- implementing Privacy by Design when Processing Personal Data and completing DPIAs where Processing presents a high risk to rights and freedoms of Data Subjects;
- integrating data protection into internal documents including this policy and any other related policies, privacy guidelines or privacy notices;
- ensuring that all people who work for us are adequately trained to enable them to comply with data privacy laws. We must maintain a record of training attendance; and
- 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.

You must regularly review all the systems and processes under your control to ensure they comply with this Policy and check that adequate governance controls and resources are in place to ensure proper use and protection of Personal Data. You should provide any information to the [DPO/DPL] as required.

17. Record Keeping

The UK GDPR requires us to keep full and accurate records of all our data Processing activities.

You should ensure that any Processing of Personal Data that you undertake is included in the records by checking with the [DPO/DPL].

18. Training And Audit

We are required to ensure all people who work for us have undergone adequate training to enable them to comply with data privacy laws. We must also regularly test our systems and processes to assess compliance.

You must undergo all mandatory data privacy-related training offered to you.

You must regularly review all the systems and processes under your control to ensure they comply with this policy and check that adequate governance controls and resources are in place to ensure proper use and protection of Personal Data.

19. Privacy By Design and Data Protection Impact Assessment (DPIA)

We are required to implement Privacy by Design measures when Processing Personal Data by implementing appropriate technical and organisational measures (like Pseudonymisation) in an effective manner, to ensure compliance with data privacy principles.

Controllers must also conduct DPIAs in respect to high-risk Processing. If you believe Processing that you are carrying out is high risk, please speak to the [DPO/ DPL].

20. Automated Processing (Including Profiling) And Automated Decision-Making

Generally, ADM is prohibited when a decision has a legal or similar significant effect on an individual unless:

1. a Data Subject has Explicitly Consented;
2. the Processing is authorised by law; or
3. the Processing is necessary for the performance of or entering into a contract.

If certain types of Special Categories of Personal Data or Criminal Convictions Data are being processed, then grounds (2) or (3) will not be allowed. However, the Special Categories of Personal Data and Criminal Convictions Data can be Processed where it is necessary (unless less intrusive means can be used) for substantial public interest like fraud prevention.

If a decision is to be based solely on Automated Processing (including profiling), then the Data Subject must be informed when you first communicate with them of their right to object. This right must be explicitly brought to their attention and presented clearly and separately from other information. Further, suitable measures must be put in place to safeguard the Data Subject's rights and freedoms and legitimate interests.

We must also inform the Data Subject of the logic involved in the decision making or profiling, the significance and the envisaged consequences, and give the Data Subject the right to request human intervention, express their point of view or challenge the decision.


A DPIA must be carried out before any Automated Processing (including profiling) or ADM activities are undertaken.

21. Direct Marketing

We are subject to certain rules and privacy laws when engaging in direct marketing to our [customers/ donors/ supporters/ volunteers / members] and prospective [customers/ donors/ supporters/ volunteers / members].

For example, in a business to consumer context, a Data Subject's prior consent is generally required for electronic direct marketing (for example, by email, text or automated calls). The limited exception for existing customers known as "soft opt-in" allows an organisation to send marketing texts or emails without consent if it:

- Has obtained contact details in the course of a sale to that person.
- Is marketing similar products or services.
- Gave the person an opportunity to opt out of marketing when first collecting the details and in every subsequent marketing message.



The right to object to direct marketing must be explicitly offered to the Data Subject in an intelligible manner so that it is clearly distinguishable from other information.

A Data Subject's objection to direct marketing must always be promptly honoured. If an individual opts out of marketing at any time, their details should be suppressed as soon as possible. Suppression involves retaining just enough information to ensure that marketing preferences are respected in the future.

22. Policy Version

This policy was adopted on [].

Data Retention: Guidelines for retention of HR Data

Data Retention: Guidelines for retention of HR Data

This guidance note accompanies the Data Retention: Guidelines for Retention of HR Policy Template and is designed to provide drafting assistance to those implementing the policy. It outlines key considerations, best practice and practical advice to ensure the policy is effectively and consistently applied.

*** Please note the following in respect of the Data Retention: Guidelines for Retention of HR Policy Template:**

- The template contains square brackets and highlighting to show the areas you will need to insert information and/or consider whether the options shown are relevant to your organisation. Your review should not be limited to these areas, as there may be areas in the template that are not relevant to your organisation and should be deleted.
- The template deals with retention periods for HR data. The same format of document can be used for all different types of personal data. The important thing is to identify the relevant categories of personal data and establish the period for which they should be kept.
- When you have finalised your guidelines, you should remove all the square brackets and highlighting.
- There are recommended retention periods for HR data in these guidelines. These do not constitute legal advice and may not be relied on for that purpose. Your organisation should take separate legal advice if it unsure how long personal data should be retained.

Clause	Guidance
1.3	This should be the person who has been designated to oversee Data Protection matters for your organisation. You may use the job title rather than a name.
4	Amend as appropriate for the individual. Again, include the most applicable option and details – e.g. can employees update this information automatically using an online portal that you may have, or would they need to notify a designated person?
7.2	12 months is recommended but this should reflect what you currently do in practice if a candidate for employment is not successful. This position is also reflected in the table below.
Clause 8	<p>This table contains examples of categories of information that you are likely to collect from employees. Please remove any that are irrelevant and add in any other categories of information that you wish to include in the table. We have made some suggestions/recommendations in relation to the retention periods for you to review and consider.</p> <p>As there is the possibility that any documents relating to a worker/ employee could be relevant to a Tribunal, County Court or High Court claim, employers may consider it appropriate in particular cases to retain relevant records for up to seven years after termination of employment. That takes account of the six-year limitation period and includes a further year for claims that have been brought to reach the employer. In some cases longer periods may be appropriate.</p> <p>In the following cases, there are statutory minimum retention periods:</p> <ul style="list-style-type: none"> • Immigration checks: two years after the termination of employment (section 15(7)(c), Immigration, Asylum and Nationality Act 2006 and article 6(b), Immigration (Restrictions on Employment) Order 2007 (SI 2007/3290)). • PAYE records: at least three years after the end of the tax year to which they relate (regulation 97, Income Tax (Pay As You Earn) Regulations 2003 (SI 2003/2682)). • Payroll and wage records for companies: six years from the financial year-end in which payments were made (paragraph 21, Schedule 18, Finance Act 1998). • Payroll and wage records for unincorporated business: five years after 31 January following the year of assessment (section 12B, Taxes Management Act 1970). • Records in relation to hours worked and payments made to workers: six years beginning with the day on which the pay reference period immediately following that to which they relate ends (section 9, National Minimum Wage Act 1998 and regulation 59, National Minimum Wage Regulations 2015 (SI 2015/621) as amended by the National Minimum Wage (Amendment) Regulations 2021 (SI 2021/329)). • Records required by the Working Time Regulations 1998 (SI 1998/1833) (WTR): • Working time opt out: two years from the date on which they were entered into (regulations 5 and 9, WTR). • Compliance records: two years after the relevant period (regulations 5, 7 and 9, WTR). • Maternity records: three years after the end of the tax year in which the maternity pay period ends (regulation 26, Statutory Maternity Pay (General) Regulations 1986 (SI 1986/1960)). • Accident records: at least three years from the date the report was made (Schedule 1, Part II, Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 2013 (SI 2013/1471)).

Clause	Guidance
Clause 8	Given the possible ongoing relevance of some of these records, in certain cases an employer may consider it appropriate to retain records for seven years after termination of employment, bearing in mind litigation risk. In other cases, a further year has been added to the statutory retention period to enable the fact of any dispute to reach the employer's attention after the statutory period has ended. In the case of recruitment documents, given that the time limit for likely claims is the three-month tribunal time limit, an extension to 12 months allows for pre-claim conciliation and for the claim to reach the employer after it has been presented to an employment tribunal.
Clause 8 (table-pension Records)	This section is aimed at the record-keeping requirements relating to pension records. The majority of retention periods recommended are based on minimum statutory retention periods
Clause 8 (table-auto-enrolment opt-in notices and joining notices / opt-out notices)	Opt-in notices, joining notices and opt-out notices must be kept in the original format, although copies of the original format or electronically stored versions are acceptable.

Sample Policy: Data Retention: Guidelines for retention of HR Data

USING THESE GUIDELINES

- * Using this template – this template contains square brackets and highlighting to show the areas you will need to insert information and/or consider whether the options shown are relevant to your organisation. Your review should not be limited to these areas, as there may be areas in the template that are not relevant to your organisation and should be deleted.*
- * This template deals with retention periods for HR data. The same format of document can be used for all different types of personal data. The important thing is to identify the relevant categories of personal data and establish the period for which they should be kept.*
- * When you have finalised your guidelines, you should remove all the square brackets and highlighting.*
- * There are recommended retention periods for HR data in these guidelines. These do not constitute legal advice and may not be relied on for that purpose. Your organisation should take separate legal advice if it unsure how long personal data should be retained.*

ABOUT THESE GUIDELINES

This policy provides information about the data protection legislation, including the UK General Data Protection Regulation ("UK GDPR") and Data Protection Act 2018 with which [Organisation Name] ("the Organisation", "we", "our", "us") must comply.

- 1.1** These guidelines support [Organisation's] (we/us) data protection policy.
- 1.2** The guidelines are intended to ensure that [Organisation] processes process personal data in the form of employment records in accordance with the personal data protection principles, in particular that:
 - 1.2.1** Personal data must be collected only for specified, explicit and legitimate purposes. It must not be further processed in any manner incompatible with those purposes.
 - 1.2.2** Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed. When personal data is no longer needed for specified purposes, it is deleted or anonymised as provided by these guidelines.
 - 1.2.3** Personal data must be accurate and, where necessary, kept up to date. It must be corrected or deleted without delay when inaccurate.
 - 1.2.4** Personal data must not be kept in an identifiable form for longer than is necessary for the purposes for which the data is processed.
 - 1.2.5** Personal data must be secured by appropriate technical and organisational measures against unauthorised or unlawful processing, and against accidental loss, destruction or damage.
- 1.3** The [DESIGNATION] is responsible for overseeing these guidelines. Any questions about the operation of the guidelines should be submitted to [DESIGNATION].

2. LOCATION OF EMPLOYMENT RECORDS

- 2.1 [DESIGNATION] holds employment records and can be contacted with any enquiries relating to your personal data.

3. KEEPING INFORMATION UP TO DATE

- 3.1 We need to ensure that your personal details are up to date and accurate.

4. When you first start working for us we record [your name] [address] [next of kin] [and] [contact telephone details]. In the event that any of these change you should [update your details on [DETAILS OF ONLINE ACCESS] OR inform [DESIGNATION]]. You will be invited to review and update personal data on a regular basis.

5. These provisions are intended to complement the data subject rights referred to in the Data Protection Policy.

6. GENERAL PRINCIPLES ON RETENTION AND ERASURE

- 6.1 [Organisation]'s approach to retaining employment records is to ensure that it complies with the data protection principles referred to in these guidelines and, in particular, to ensure that:

- 6.1.1 Employment records are regularly reviewed to ensure that they remain adequate, relevant and limited to what is necessary to facilitate you working for us.
- 6.1.2 Employment records are kept secure and are protected against unauthorised or unlawful processing and against accidental loss, destruction or damage. Where appropriate we will use anonymisation to prevent identification of individuals.
- 6.1.3 When records are destroyed, whether held as paper records or in electronic format, we will ensure that they are safely and permanently erased.

7. RETENTION AND ERASURE OF RECRUITMENT DOCUMENTS

- 7.1 We retain personal data following recruitment exercises to demonstrate, if required, that candidates have not been discriminated against on prohibited grounds and that recruitment exercises are conducted in a fair and transparent way.
- 7.2 Personal data that is collected by us during the recruitment process is likely to be retained for [twelve months] from the communication of the outcome of the recruitment exercise which takes account of both the time limit to bring claims and for claims to be received by us.
- 7.3 Information relating to successful candidates will be transferred to their employment record with us. This will be limited to that information necessary for the working relationship and, where applicable, that required by law.
- 7.4 Following a recruitment exercise information, in both paper and electronic form, will be held by [DESIGNATION]. Destruction of that information will take place in accordance with these guidelines.

8. RETENTION AND ERASURE OF EMPLOYMENT RECORDS

8.1 [Organisation] has regard to recommended retention periods for particular employment records set out in legislation, referred to in the table below. However, it also has regard to legal risk and may keep records for up to seven years (and in some instances longer) after your employment or work with us has ended.

Type of employment record	Retention period
Recruitment records	
<p>These may include:</p> <p>Completed online application forms or CVs.</p> <p>Equal opportunities monitoring forms.</p> <p>Assessment exercises or tests.</p> <p>Notes from interviews and short-listing exercises.</p> <p>Pre-employment verification of details provided by the successful candidate. For example, checking qualifications and taking up references. (These may be transferred to a successful candidate's employment file).</p> <p>Criminal records checks. (These may be transferred to a successful candidate's employment file if they are relevant to the ongoing relationship).</p>	Twelve months after notifying candidates of the outcome of the recruitment exercise.
Immigration checks	Three years after the termination of employment.
Contracts	
<p>These may include:</p> <p>Written particulars of employment.</p> <p>Contracts of employment or other contracts.</p> <p>Documented changes to terms and conditions.</p>	While employment continues and for seven years after the contract ends.
Collective agreements	
Collective workforce agreements and past agreements that could affect present employees.	Any copy of a relevant collective agreement retained on an employee's record will remain while employment continues and for seven years after employment ends.
Payroll and wage records	
<p>Details on overtime.</p> <p>Bonuses.</p> <p>Expenses.</p> <p>Benefits in kind.</p>	These must be kept for at least three years after the end of the tax year to which they relate. However, given their potential relevance to pay disputes they will be retained for seven years after employment ends.

Type of employment record	Retention period
Payroll and wage records	
Current bank details	Bank details will be deleted as soon after the end of employment as possible once final payments have been made.
PAYE records	These must be kept for at least three years after the end of the tax year to which they relate. However, given their potential relevance to pay disputes they will be retained for seven years after employment ends.
[Payroll and wage records for companies] or [Payroll and wage records for unincorporated associations]	<p>[These must be kept for six years from the financial year-end in which payments were made. However, given their potential relevance to pay disputes they will be retained for seven years after employment ends.]</p> <p>Or</p> <p>[These must be kept for five years after 31 January following the year of assessment. However, given their potential relevance to pay disputes they will be retained for seven years after employment ends.].</p>
Records in relation to hours worked and payments made to workers	These must be kept for three years beginning with the day on which the pay reference period immediately following that to which they relate ends. However, given their potential relevance to pay disputes they will be retained for seven years after the working relationship ends.
Travel and subsistence.	While employment continues and for seven years after employment ends.
Record of advances for season tickets and loans to employees	While employment continues and for seven years after employment ends.
Personnel records	
<p>These include:</p> <p>Qualifications/references.</p> <p>Consents for the processing of special categories of personal data.</p> <p>Annual leave records.</p> <p>Annual assessment reports.</p> <p>Disciplinary procedures.</p> <p>Grievance procedures.</p> <p>Death benefit nomination and revocation forms.</p> <p>Resignation, termination and retirement.</p>	While employment continues and for seven years after employment ends

Type of employment record	Retention period
Records in connection with working time	
Working time opt-out	Three years from the date on which they were entered into.
Records to show compliance, including: Time sheets for opted-out workers. Health assessment records for night workers.	Three years after the relevant period.
Maternity, Paternity, Adoption and Shared Parental Leave ("collectively referred to as family leave records").	
These include: Details of payments made during family leave. Dates of family leave. Period without any payment for family leave. Maternity certificates showing the expected week of confinement.	Four years after the end of the tax year in which the maternity pay period ends.
Accident records	
These are created regarding any reportable accident, death or injury in connection with work.	For at least four years from the date the report was made.
Medical information/ records	
These include: Medical questionnaires. Records of sickness absence including medical certificates. Annual medical checks. Medical reports obtained from occupational health	While employment continues and for seven years after employment ends.
Pension records	
Name and address of scheme or provider of the automatic enrolment scheme used to comply with the employer's duties.	For six years starting from the day on which the record must first be kept.
Employer pension scheme reference.	For six years starting from the day on which the record must first be kept.
Evidence scheme complies with auto-enrolment statutory quality tests.	For six years starting from the day on which the record must first be kept.

Type of employment record	Retention period
Pension records	
Name, NI number, date of birth and automatic enrolment date of all jobholders auto-enrolled (and corresponding details for non-eligible jobholders and entitled workers who have opted in or joined).	For six years starting from the day on which the record must first be kept.
Evidence of jobholders' earnings and contributions.	For six years starting from the day on which the record must first be kept.
Contributions payable by employer in respect of jobholders and dates on which such contributions were paid to scheme.	For six years starting from the day on which the record must first be kept.
If auto-enrolment postponement period used, records of workers who were given notice of postponement including full name, NI number and date postponement notice was given.	For six years starting from the day on which the record must first be kept.
Auto-enrolment opt-in notices and joining notices (original format).	For six years starting from the day on which the record must first be kept.
Opt-out notices (original format).	For four years starting from the day on which the record must first be kept.
If employer is (or was) a sponsoring employer of an occupational pension scheme, any document relating to monies received by or owing to the scheme, investments or assets held by the scheme, payments made by the scheme, contracts to purchase a lifetime annuity in respect of scheme member and documents relating to the administration of the scheme.	For the tax year to which they relate and the following 6 years.
Information relating to applications for ill health early retirement benefits, including medical reports.	While entitlement continues and for a period of 15 years after benefits stop being paid.
Death benefit nomination and revocation forms.	While entitlement continues and for period of 15 years after the death of member and their beneficiaries.

Data Protection Impact Assessment

Data Protection Impact Assessment (DPIA)

Article 35 of the UK General Data Protection Regulation (UK GDPR) introduces a formal requirement for organisations, in their role as data controllers, to conduct a data protection impact assessment (DPIA) before undertaking any processing that presents a specific privacy risk by virtue of its nature, scope or purposes.

Undertaking a DPIA should be thought of as a process. This standard document is a template to be used to draw together information gathered through the DPIA process, to document the outcome of the DPIA and to record the actions to be taken as a result of the DPIA.

When completing the DPIA you should complete the fact-gathering sections first before completing the analysis sections (in particular, Section 7), with the executive summary (Section 1) being the final section to be completed.

You should consult [] our data protection [officer (DPO) / lead] before finalising this document. You may also find it helpful to refer to the ICO guidance on conducting DPIAs. In some circumstances, we may need to share the DPIA with the ICO.

<https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/data-protection-impact-assessments-dpias/>



This guidance is to be used by the recipient only and should not be passed to third parties without our consent”.

You should assess privacy risk from the data subject's perspective. A key consideration of the DPIA is to determine what needs to be done to keep the data subject's personal data safe. Where there is risk to a data subject there is likely to be risk to the controller, in particular legal and regulatory compliance risks. Whilst a DPIA should primarily concern the risks posed to data subjects by the initiative, the scope should also consider risks to the controller and other stakeholders, including society at large. From the organisational perspective, any financial, legal, reputational and other relevant risks should be considered as part of this process.

The information in these boxes is for guidance only and should be deleted from the final document.

Document history:

This DPIA is a living document to record the analysis undertaken, decisions made and steps to be taken in relation to an initiative. It should be updated on a regular basis and therefore includes a document version management table. It may be sensible to nominate one individual as the document owner, who has overall responsibility for the DPIA and keeps a record of all individuals who have been asked to review the DPIA with details of versions reviewed.

Document history:

Version number	Summary of change	Reviewer	Date

1. Executive Summary

This section should record at a high level the key facts from the assessment as well as the conclusions drawn. The section should include:

- A high level description of the initiative.
- A summary of the processing scope.
- A summary of the purposes for which processing will occur.
- A summary of the intended benefits for data subjects, third parties and the data controller.
- A summary of the rationale as to why a DPIA is required.

The “Summary: rationale as to why a DPIA is required” box should be completed as quickly as possible. However, the remainder of this Section 1 should be among the last pieces of the DPIA to be completed. Note that if a conclusion is reached that a DPIA is not required, controllers may still wish to record the fact that they considered a DPIA and determined that it was not needed in the circumstances, with the rationale as to why they reached this conclusion.

High level description of the initiative:

[Summarise from Section 3 of the DPIA.]

Summary: scope of processing:

[Summarise from Section 5 of the DPIA.]

Summary: purposes for which processing will occur:

[Summarise from Section 8 of the DPIA.]

Summary: intended benefits for data subjects, third parties and the organisation:

[Summarise from Section 8 of the DPIA.]

Summary: rationale as to why a DPIA is required:

[Summarise from Section 3 of the DPIA.]

2. Administrative Information

This section sets out who has been involved with the initiative and other key logistical information.

If there are any other key stakeholders you should consider identifying these here. Also consider whether this section needs to be personalised to refer to any particular risk management processes of any of those stakeholders as well as to the individual/committee ultimately responsible for taking decisions about what risks are acceptable for the organisation.

Name of Initiative:

[Initiative/Initiative name]

Name and role of organisation completing the DPIA:

[Organisation name Controller/Processor]

Area responsible for the Initiative:

[For example, IT, HR, Finance, Fundraising]

Senior executive responsible for the Initiative:

Name:

Email address:

Mobile phone/direct dial:

Initiative project manager:

Name:

Email Address:

Mobile Phone/Direct Dial:

Data Protection Officer:

Name:

Email address:

Mobile phone/direct dial:

Other stakeholders: Name:

Email address:

Mobile phone/direct dial:

Other stakeholders: Name:

Email address:

Mobile phone/direct dial:

Third parties involved/associated with the Initiative

[These are as listed in Section 10]/[None]

Relevant documents

[Identify relevant documents and consider including copies as an Annex.]

[Initiative/Initiative business case]

[Design documents]

[Previous DPIAs]

[DPIAs covering related processing operations]

[Documents to refer to: Privacy policy, Relevant legislation, ICO Guidance, WP29 DPIA Guidance, European Data Protection Board Guidelines, Codes of Conduct, Other policies: [for example, Information security, Data retention, HR, Marketing, Finance, appropriate policy document for special categories of personal data and criminal convictions].]

3. Overview

This section should provide context and information to the reader on how the DPIA fits in with the Initiative. It should provide a high level description of the Initiative and explain how the scope of the DPIA relates to the Initiative. Identify the context of the Initiative – it may be a pilot or may be a phase of a project or programme. There may also be related processing activities which are relevant and, if so, these should be mentioned.

This section should also be used to describe the key parameters of the DPIA so that it is clear what is in scope and what has been excluded (perhaps to be undertaken under a separate DPIA). Note that the key parameters of the DPIA may be different from the key parameters of the Initiative.

In this section you should also identify why a DPIA has been conducted.

If the DPIA covers multiple sets of processing operations, identify them here and record the rationale as to why the processing operations are regarded as similar.

High level description of the Initiative:

[In this section include a high level description of the Initiative, so that it is easy to then explain the scope of the DPIA in the context of the overall initiative.]

Relationship between the DPIA and the Initiative:

[Explain the scope of the DPIA in the context of the overall initiative.]

Context:

[Consider:

Pilot

Phase

Initiative vs Programme

Related processing activities]

Key parameters (for example, boundaries of DPIA). What is in scope and excluded from scope?:

[It may be useful to describe the boundary lines of the DPIA and what is covered by the assessment. Note that this may be different to the boundary of the Initiative.]

Rationale as to why a DPIA is required:

[Processing is high risk, [explain why].]

Multiple sets of data processing operations:

[If the DPIA covers multiple sets of data processing operations provide further explanation here.]

4. Consultation

This section should summarise the advice and input from all stakeholders and interested parties that have been consulted in relation to the DPIA. This will include the functional area or business unit carrying out the DPIA and the DPO (if there is one).

It will also comprise the advice and input of the data subjects, their representatives and other interested stakeholders as well as professional experts such as lawyers, IT experts, security experts, sociologists and ethics experts.

Advice of DPO:

[Advice obtained from the DPO (Ref Annex D)]

Input of specific business functions:

[Record the advice/input of specific business functions that are stakeholders/have an interest in the Initiative.]

Input of data subjects and/or their representatives:

[Explain how the views were sought. For example, obtained through studies, questionnaires, discussion with data subject representatives and what the views were.]

[Final decision – if different from Data subject's views to include rationale for proceeding.]

[Justification for not seeking input from Data subjects for example, compromises confidentiality of business plans, disproportionate, impractical.]

Input of experts and other interested stakeholders:

[Record the advice/input of independent experts of different professions (such as lawyers, IT experts, security experts) as well as other stakeholders who have an interest in the Initiative.]

Consultation with the ICO:

[If consultation required, summarise output and decisions made. Include any advice of ICO as an annex to the DPIA.]

5. Scope

This section should be used to detail the facts about the Initiative. Most DPIAs will involve or be triggered by the introduction of new systems or technology or changes to them. However, look more widely than just the technology and consider all elements that may be involved in the Initiative including the people and processes.

Identify the type(s) of data subject that is involved – it is important to be clear, in the factual sense, as to what type of data is under consideration.

Description:

[Description of Initiative including technical capabilities/functionality]

Assets/technology involved with processing the personal data:

- a. Hardware
- b. Software
- c. Networks
- d. People
- e. Paper
- f. Paper Transmission Channel(s)
- g. Mobile Devices
- h. Cookies
- i. Other such as cloud, data warehouses etc.

Business context:

[It is often useful to explain the background/business context to the Initiative. This will also help when discussing the objectives and benefits of the processing.]

Types of data subject:**Initiative's objectives and scope:**

[To be confirmed – this section may be merged with Business context above.]

6. Description of Processing

This section is the core of the DPIA. Build upon the facts gathered and documented earlier in the DPIA and focus in on the types of data involved and nature of the processing operations. It may be useful to create a data flow map as part of this element. The data flow map should be included in an annex to the DPIA.

When describing the data processing operations it is useful to consider:

The types of personal data.

The sources of the personal data (such as whether it is from feeds from internal/external systems, purchased lists or collected directly from data subjects).

The length and frequency of processing.

The processing volumes.

The approach that has been/will be taken to data minimisation.

Data flow map(s):

[See Annex A.

Data entry and exit points, location, user categories, data subject categories]

Description of the proposed processing operations:

[To be confirmed – this section may be merged with Description in the Scope section, Section 5 above]

Types of personal data:

[Identification of categories/types of personal data collected]

Sources of the personal data:

[- Feeds from systems (internal/external)

- - Collected directly from data subjects]

Length and frequency of processing:

Processing volumes:

[Volumes – Data subjects and records

Volumes of certain types of data subject (such as children; vulnerable individuals) Volumes

– users and type

Type of users – internal, external (such as affiliates, vendors and alliance partners)]

Data minimisation:

[Identify considerations given to data minimisation (such as certain types of data subject not included in scope, types of data/fields collected minimised, data flows minimised, de-identification techniques used).]

7. Basis of Processing

This is another key section that goes to the heart of the requirements under Article 35(7). The data controller should be carrying out two key assessments:

Necessity and proportionality assessment. This is an assessment of the necessity and proportionality of the processing operations in relation to the purpose(s) of the processing (Purpose(s)).

Rights and freedoms assessment. This is an assessment of the risks to the rights and freedoms of the data subjects.

When completing the rights and freedoms assessment the primary concern is for the right to privacy but there are also other fundamental rights (including freedom of speech, freedom of thought, freedom of movement, prohibition of discrimination, right to liberty, conscience and religion) and regard should be had to all of these.

It is also important to address fair and transparent processing requirements. A copy of the data controller's privacy notice(s) (or a link to it) should be included in an annex to the DPIA.

Lawful processing

Necessity and proportionality assessment (assessment of the necessity and proportionality of the processing operations in relation to the Purpose(s)): [Purpose limitation:

- Specified, explicit and legitimate purposes(s)
- Lawfulness of processing
- Grounds
- Consent
- Legitimate interest

1. Balancing test – assess whether legitimate interests are overridden by the interests or fundamental rights and freedoms of the data subjects
 2. Adequate, relevant and limited to what is necessary
 3. Limited storage duration
- Measures contributing to the rights of the data subjects

Rights and freedoms assessment (assessment of the risks to the rights and freedoms of the data subjects):

Fair processing:

[Fair processing requirements:

1 Information provided to the data subject (privacy notice) 2 Use of cookies]

8. Purpose(S) of Processing; Benefits and Risks

The section is intended to focus on the purpose for which personal data is processed and to assess the intended benefits and risks. The UK GDPR does not define "high risk" but does require that an assessment is carried out "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".

Any of the following categories of processing should be assessed in more detail to establish whether such processing is high risk:

- Automated processing (including profiling).
- Evaluation or scoring (including profiling or predicting).
- Automated decision-making with legal (or similar) effect.
- Large-scale processing of data.
- Processing of sensitive data or data of a highly personal nature.
- Systematic monitoring of publicly accessible area(s).
- Creation or use of personal profiles.
- Matching/combining datasets.
- Processing in relation to vulnerable data subjects.
- Innovative use or applying new technologies or innovative solutions.
- Processing which, in itself, "prevents data subjects from exercising a right or using a service or a contract".

As part of the assessment, you should identify the benefits that may result from the processing. When doing so, consider the position holistically. Benefits could be to: (i) individuals (data subjects and users); (ii) groups of individuals; and (iii) organisations such as the data controller/third parties; and/or (iv) wider society.

Also consider the risks associated with the processing, including to the data subjects, the data controller itself and any other relevant stakeholders. Identify the type of risk, possible threats and sources of risk, the likelihood of risk occurring and the impact of the risk and the type of damage. Within this section, include any risks associated with not proceeding with the Initiative.

Finally, but of utmost importance, also consider the risk mitigation options. Bear in mind that the quality and sufficiency of the risk mitigation steps that can be taken will impact on the need to consult with the ICO.

Purpose(s) of processing

[Automated processing (including profiling)

Evaluation or scoring (including profiling or predicting) Automated decision making with legal (or similar) effect Large scale processing of data

Sensitive data or data of a highly personal nature Systemic monitoring of publicly accessible area Creation or use of personal profiles Matching/combining datasets

Vulnerable data subjects

Innovative use or applying new technologies or innovative solutions

Processing in itself “prevents data subjects from exercising a right or using a service or a contract

Other [marketing, analytics]

Benefits

[Individual(s) [Data subjects, users] Group of individuals

Organisation(s) [Data controller, third parties] Society]

Risks

[Types of risk

Possible threats/sources of risk (Recital 90) Likelihood of risk occurring

Impact if risk occurs/type of damage/ severity of harm

Risk mitigation options and effect on risk]

9. Transfers outside the UK

A component of the DPIA is to consider any potential transfers of data from the UK. As a starting point, it is useful to identify the key countries that the data will "touch". Consider the countries where the data subject is located as well as the countries that any users are located. Also identify where key processing activities occur. For example, does the processing involve use of a cloud solution? Where does storage, back up and disaster recovery occur? Where does support and maintenance occur (whether technology support or customer support)? If there are a number of countries involved then it is necessary to consider your international data transfer arrangements.

The conditions for transferring personal data outside the UK and making a restricted transfer of data are found at Chapter V of the UK GDPR.

There are essentially two avenues available to organisations seeking to make a restricted transfer from the UK: either the transfer is made into a country which is the subject of UK adequacy regulations or the parties have put another transfer safeguard mechanism in place to make sure the data remains secure.

Legal advice should be sought if you are unsure whether you meet the conditions for transferring personal data outside the UK.

Country summary:	
Location of data subjects:	
Location of users:	[Consider: Employees Contractors Third Parties]
Hosting location:	
Support and maintenance:	[Consider application support and maintenance but also customer support]
Country specific documents:	[See Annex e.g. Local language privacy notices]
International data transfer arrangements:	
Name and role of parties receiving the personal data:	
Grounds for transfer:	[Binding Corporate Rules UK Standard contractual clauses (IDTA or Addendum) Other]

10. Disclosure to Third Parties

It is important to identify any third parties, whether other data controllers or data processors, that will handle the personal data. Consider the following questions as part of the analysis for each recipient:

- Where is the recipient located?
- What is the recipient's role (controller or processor) with regard to the data?
- What data is to be disclosed to them and why?
- Does all of the data identified for disclosure need to be disclosed? (In other words, what data minimisation steps can be taken?)
- What agreements need to be put in place with the recipients?
- Is a separate DPIA required?
- What monitoring/contract management arrangements need to be put in place?

Recipients:

Name:

Address:

Role:

Data to be disclosed Role of the recipient Reasons for disclosure Agreements

Need for separate DPIA?

Monitoring arrangements/contract management

11. Security of Processing

In this section you should address the technical and organisational measures, including practical safeguards and technical security measures, to ensure the data is kept secure.

Consider practical measures such as identity and access management arrangements, training, communication and awareness, third party due diligence arrangements and third party contract management and monitoring arrangements.

Consider the range of technical security measures that can be implemented such as encryption, pseudonymisation and two-factor authentication. Ensure that arrangements for data security breach notification have been considered.

Record items such as steps taken for de-identification of data, arrangements for destruction of data and data back up and disaster recovery arrangements. Include records in relation to consents, privacy notices, data flow maps and approvals.

Practical safeguards:

[Examples: Identity and access management arrangements Examples: Training, communication and awareness Examples: Due diligence arrangements re: third parties Examples: Contract management and monitoring arrangements with third parties]

Security measures:

[Examples: Encryption
Examples: Arrangements re: data security breach notification]

Mechanisms to protect personal data:

[Examples: De-identification of data
Examples: Arrangements re destruction of data Examples: Data back up/disaster recovery arrangements]

Mechanisms to demonstrate compliance with legislation:

[Examples: Maintenance of records such as re: consents, privacy notices, data flow maps, approvals.]

12. Data Quality

To ensure compliance with the data protection principles it is important to ensure that data sets are comprehensive, complete, without bias and accurate. Put in place arrangements for the regular review of data sets and to keep information up to date.

Assessment of quality:

[Checking that data sets are comprehensive, complete, without bias, accurate. Balancing with the need for data minimisation.]

Review arrangements:

[Arrangements to review the data sets and to keep information up to date and accurate.]

13. Retention and Disposal

In this section consider issues associated with how the storing and holding of data will occur, the period of time it will be retained and how it will be deleted. Particular areas to consider are:

- Retention periods.
- Arrangements for archive and back up.
- Disaster recovery and business continuity arrangements.
- System decommissioning.

Retention periods:

[Identify how long the different types of data will be stored for.]

Archiving:

Back-up:

Business continuity:

System decommissioning:

[Identify any systems which need decommissioning. Consider associated issues such as data migration and secure data deletion.]

14. Special Arrangements for Vulnerable Individuals

In this section consider whether any special arrangements for vulnerable individuals are required. Information on this topic may be dispersed throughout the DPIA but it is useful to bring all the information together in one section to allow a holistic look at the overall arrangements.

Category of vulnerable individuals:

[Look for instances of imbalance of power between the data controller and data subject and identify types of individuals involved where this exists.]

Special arrangements required:

[What arrangements, if any, are required? Examples might be special arrangements for consent, or adjustments to privacy notices.]

15. Actions

This section is intended to draw together all the actions that need to be taken in order to implement the risk mitigation steps that have been identified. To ensure that actions get completed, each action should be allocated to a specific owner with a date at which the allocation was made and a proposed date for completion.

Action required	Owner	Date identified	Date to be completed

16. Decision

This section records the final decision taken in relation to the DPIA. This should be completed by individual(s) with sufficient overall authority such as the head of privacy, a senior lawyer or compliance officer and/or the head of the business unit behind the Initiative. The data controller may decide to:

proceed with the Initiative on the basis of the findings of the DPIA;
not proceed with the Initiative; or
seek approval from the ICO before proceeding with the Initiative.

Decision:

[Proceed with Initiative/Not proceed with Initiative/Seek approval from ICO/Other]

Rationale:

DPO advice accepted or overruled (and if overruled, reasons for this):
Authorised person:

Annex A:
Relevant Documents

Annex B:
Data Flow Map(s)

Annex C:
Privacy Notice(s)

Annex D:
DPO advice

Annex E:
Country-specific documents

Annex F:
**Other (e.g. correspondence
with Information Commissioner)**

If you require further information please contact:

Third Sector Support Wales