Churches Together in England

DATA PROTECTION POLICY

1. Introduction
	1. Churches Together in England (CTE) holds personal data about job applicants, employees, volunteers, contracted workers, members, suppliers and other individuals for a variety of purposes.
	2. CTE recognises that the correct and lawful treatment of personal data will maintain confidence in the organisation and will provide for successful operations. Protecting the confidentiality and integrity of personal data is a critical responsibility that we take seriously at all times.
	3. This policy sets out how CTE seeks to protect personal data and ensure staff understand the rules governing their use of personal data to which they have access in the course of their work.
	4. This policy applies to all personal data CTE processes regardless of the media on which that data is stored or whether it relates to past or present employees, volunteers, contracted workers, members, suppliers or any other individuals.
	5. This policy requires the General Secretary to ensure that appropriate professional legal advice is sought before any significant new data processing activity is initiated, to ensure that relevant compliance steps are addressed, and at other times when further clarification is required.
	6. The General Secretary is responsible for the monitoring and implementation of this policy. If any questions arise about the content or implementation of this policy contact should be made with the General Secretary. In particular, staff **must always** contact the General Secretary in the following circumstances:
		1. It is unclear which lawful basis should be relied upon to process personal data (including the legitimate interests used by CTE (see section 5.2 below);
		2. It is necessary to rely on consent and/or explicit consent to process personal data (see section 13 below);
		3. It is necessary to draft a Privacy Notice (see section 5.10 below);
		4. If the retention period for the personal data being processed is unclear or unknown (see section 9 below);
		5. It is unclear what security or other measures need to be implemented to protect personal data (see section 10 below);
		6. Personal data is being transferred outside the EEA (see section 14 below);
		7. If there has been a personal data breach (section 18 below);
		8. Whenever there is a significant change in processing activity or new processing activity in relation to personal data (this may require a Data Protection Impact Assessment) (see section 12 below);
		9. It is intended that personal data will be used for a purpose other than that for which it was collected.

**Scope**

* 1. This policy applies to all staff, which for these purposes includes employees, trustees, temporary, contract and agency workers, other contractors, interns and volunteers.
	2. All staff must be familiar with this policy and comply with its terms.
	3. Compliance with this policy is mandatory. Staff must also comply with any related policies and privacy notices. Any breach of this Data Protection Policy may result in disciplinary action.
	4. CTE may supplement or amend this policy by additional policies and guidelines from time to time.
1. Definitions
	1. In this policy:
		1. **Personal data** means information relating to identifiable individuals, such as job applicants, current and former employees, agency, contract and other staff, members, clergy, suppliers and other individuals. This includes expression of opinion about the individual and any indication of someone else’s intentions towards the individual.
		2. **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. Personal data relating to criminal offences and convictions should also be treated as special category personal data.
		3. **Processing data** 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.
2. General principles
	1. CTE’s policy is to process personal data in accordance with the applicable data protection laws and rights of individuals as set out below.
	2. CTE will observe the following principles in respect of the processing of personal data, ensuring that personal data is:
		1. Processed lawfully, fairly and in a transparent manner (‘Lawfulness, Fairness and Transparency’).
		2. Collected only for specified, explicit and legitimate purposes (‘Purpose Limitation’).
		3. Adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed (‘Data Minimisation’).
		4. Accurate and where necessary kept up to date (‘Accuracy’).
		5. Not kept in a form which permits identification of individuals for longer than is necessary for the purposes for which the data is processed (‘Storage Limitation’).
		6. Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage (‘Security, Integrity and Confidentiality’).
	3. CTE is responsible for and must be able to demonstrate compliance with the data protection principles listed above (the ‘Principle of Accountability’).
3. Lawfulness, Fairness and Transparency
	1. Personal data must be processed lawfully, fairly and in a transparent manner in relation to the individual.

**Lawfulness**

* 1. CTE must ensure that there is a legal basis for processing personal data. The legal bases for processing are as follows:
		1. the individual has given his or her consent (see 13 below);
		2. the processing is necessary for the performance of a contract with the individual;
		3. to meet CTE’s legal compliance obligations;
		4. to protect the individual's vital interests;
		5. for the performance of a task in the public interest;
		6. to pursue CTE’s legitimate interests, where these interests are not overridden because the processing prejudices the interests or fundamental rights and freedoms of the individual(s). The purposes for which we process personal data for legitimate interests need to be set out the Privacy Notices (see section 5.10 below).
	2. If staff are unsure what legal basis is applicable to the personal data they are processing they should contact the General Secretary.
	3. The processing of special category data (see 3.1(b) and 3.1(c) above) may require a specific, alternative legal basis for processing.
	4. Staff should contact the General Secretary for more information about the appropriate legal basis for processing special category data.

**Members, former members and individuals connected with CTE**

* 1. Staff should be aware that membership of, or association with, CTE or its Members will generate personal data which may reveal an individual’s religious or similar beliefs (i.e. may be special category data).
	2. In the majority of instances involving such special category data, the relevant legal basis for processing the personal data upon which CTE will rely is:
		1. that the processing is carried out in the course of its legitimate activities, with appropriate safeguards, by a not-for-profit body with a religious aim, on the condition that processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes, and that the personal data is not disclosed outside that body without the consent of the individuals.
	3. CTE is a not-for-profit body with a religious aim and has put appropriate safeguards in place in the form of training, and ‘Data Sharing - A Code of Practice’, and a link (<https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/a-guide-to-lawful-basis/lawful-basis-for-processing/special-category-data/>) to information in relation to the processing of such special category data. This can be found on Sharepoint.
	4. Staff should be aware that it will be necessary to have the consent of members, former members or other individuals who have regular contact with CTE to process special category personal data where personal data is transferred outside CTE e.g., to an external third party.

**Fairness & Transparency (Privacy Notices)**

* 1. Data protection law requires CTE to provide detailed, specific information to individuals about how and why their personal data is being processed. Such information must be provided through appropriate Privacy Notices.
	2. Privacy notices must be concise, transparent, intelligible, easily accessible, and in clear and plain language so that an individual can easily understand them.
	3. Whenever CTE collects personal data ***directly*** from an individual, the individual must be provided with a link to the CTE Privacy Notice containing all the information required by data protection law (including the identity of the data controller, how and why CTE will use, process, disclose, protect and retain that personal data). The Privacy Notice must be provided when the individual first provides CTE with the personal data.
	4. CTE’s Privacy Notice on the website will usually be appropriate in relation to the general purposes for which CTE collects personal data. Staff should provide the individual with a link and/or direct the individual to this Privacy Notice at the point that the personal data is collected.
	5. When personal data is collected ***indirectly*** (for example, from a third party or publicly available source), staff must provide the individual with a link to the CTE Privacy Notice on the website, including all the information required under data protection law, as soon as possible after collecting/receiving the data, and no later than the first communication with the individual or 1 month from receiving the personal data (whichever is earlier), unless this proves impossible or would involve disproportionate effort. Staff should contact the General Secretary if providing the Privacy Notice is likely to prove impossible or involve disproportionate effort. As in 5.12 above, CTE’s Privacy Notice on the website will usually be appropriate in relation to the general purposes for which CTE collects personal data from a third party or other source.
	6. Staff must also check that the personal data was collected by the third party in accordance with data protection law and on a basis consonant with CTE’s proposed processing of that personal data.
	7. Staff are required to include a link to CTE’s Privacy Notice on the website in their e-mail signature.
	8. Staff should contact the General Secretary if they believe it is necessary to draft a different privacy notice, or if they are unclear as to when a privacy notice is required.
1. Purpose limitation
	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.
	2. Staff cannot use personal data for new, different or incompatible purposes from those disclosed when the personal data was first obtained, unless staff have informed the individuals of the new purposes and legal basis being relied upon. (if this legal basis is consent, appropriate consent must be obtained (see section 13 below).
2. Data minimisation
	1. Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.
	2. Staff may only process personal data when performing job duties which require it. Staff should not collect excessive data and should ensure, to the best of their abilities, that any personal data collected is adequate and relevant for the intended purposes.
	3. Staff must ensure that when personal data is no longer needed for specified purposes, it is deleted or anonymised in accordance with CTE’s Data Retention principles (section 9 below).
3. Accuracy
	1. Personal data must be accurate and, where necessary, kept up to date. It must be corrected or deleted without delay when discovered to be inaccurate.
	2. Staff must, to the best of their abilities, ensure that the personal data CTE uses and holds is accurate, complete, kept up to date and relevant to the purpose for which it was collected. Staff must check the accuracy of any personal data at the point of collection and at regular intervals afterwards. Staff must take all reasonable steps to destroy or amend inaccurate or out-of-date personal data.
	3. Staff must ensure that personal data held by CTE relating to themselves is accurate and updated as required. If personal details or circumstances change, staff should inform the General Secretary so CTE’s records can be updated.
4. Storage limitation (data retention)
	1. Personal Data must not be kept in an identifiable form for longer than is necessary for the purposes for which the data is processed.
	2. Staff must not keep personal data, in a form which permits the identification of an individual, for longer than needed for the legitimate purpose or purposes for which CTE originally collected it.
	3. Staff will take all reasonable steps to destroy or erase from CTE’s systems all personal data that is no longer required in accordance with CTE’s Data Protection Policy. This includes requiring third parties to delete such data where applicable.
	4. Decisions relating to the retention and disposal of personal information should be taken in accordance with this policy. In particular:
		1. Appendix 1 – Disposal & Retention Checklist – to be followed (1) when determining retention periods for personal information not included in the Retention Schedule and (2) where the disposal of **any** personal information is being considered (including the relevant categories of personal information set out in the Retention Schedule)
		2. Appendix 2 - Retention Schedule – A table containing the recommended retention period for each relevant category of personal information.
	5. Staff will ensure individuals are informed of the period for which data is stored and how that period is determined in any applicable privacy notice (see 5.10 - 5.17).

**Disposal**

* 1. In circumstances where the retention period of a document containing personal information has expired, a review should be carried out prior to a decision being made to dispose of it, in accordance with the Disposal & Retention Checklist. There may be circumstances where the personal information may need to be kept for a longer period that is designated under the Retention Schedule, for example, if the information needs to be retained due to ongoing legal proceedings. If the decision to dispose of the personal information is taken, consideration should be given to the method of disposal to be used.
	2. Disposal of records and documentation containing personal information (whether hard copy or electronic) should be carried out in a way that preserves the confidentiality of the personal information.

**Hard copy records**

* 1. Hard copy records containing personal information should be placed in confidential waste bins/or shredded for collection by an approved disposal firm.

**Electronic records**

* 1. Electronic records containing personal information require disposal (including any back-up or other copies) should be deleted (i.e., wiped).
	2. CTE recognises that deleting electronic information may not always be straightforward, for example if for technical reasons it is not possible to delete the relevant personal information in isolation, without also deleting other information. In such circumstances, the personal information should be put beyond use, so that the content cannot be recoverable in any way.
	3. Personal data that has been put beyond use in this way:
		1. Should NOT be used to inform any decision in respect of any individual or in a manner that affects the individual in any way;
		2. Should NOT be given to any other organisation, nor should any other organisation be provided access to the personal information;
		3. Should be protected by appropriate technical and security measures;
		4. Should be permanently deleted when this becomes possible.
		5. Does NOT need to be provided to individuals in response to a subject access request (provided all four safeguards above are in place).
	4. Records of disposal should be maintained, and should detail:
		1. The document disposed of;
		2. The date of disposal;
		3. The reason for disposal (e.g., in compliance with the Retention Schedule);
		4. The method of disposal; and
		5. The individual who authorised the documents disposal.
1. Security integrity and confidentiality
	1. Personal data must be secured by appropriate technical and organisational measures against unauthorised or unlawful processing, and against accidental loss, destruction or damage.
	2. CTE must implement reasonable and appropriate security measures against unlawful or unauthorised processing of personal data and against the accidental loss of, or damage to, or destruction of personal data.
	3. CTE must maintain data security by protecting the confidentiality, integrity and availability of the personal data, defined as follows:
		1. Confidentiality means that only people who have a need to know and are authorised to use the personal data can access it.
		2. Integrity means that personal data is accurate and suitable for the purpose for which it is processed.
		3. Availability means that authorised users are able to access the personal data when they need it for authorised purposes.
	4. CTE will develop, implement and maintain safeguards appropriate to:
		1. its size, scope and business;
		2. its available resources;
		3. the amount of personal data that we own or maintain on behalf of others; and
		4. identified risks (including use of encryption and pseudonymisation (i.e., 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 itself kept separately and securely) where applicable).
	5. CTE will regularly evaluate and test the effectiveness of those safeguards to ensure security of its processing of personal data.
	6. Staff have a responsibility for protecting the personal data CTE holds.
	7. Staff must exercise particular care in protecting special category personal data (see 3.1(b) above) from loss and unauthorised access, use or disclosure.
	8. Staff must follow all procedures of CTE put in place to maintain the security of all personal data from the point of collection to the point of destruction. Staff may only transfer personal data to third-party service providers who agree to comply with the required policies and procedures and who agree to put adequate measures in place, as requested (see sections 14 and 15 below).
	9. Staff must comply with all applicable aspects of the CTE’s Internet and Email Usage Policy and comply with and not attempt to circumvent the administrative, physical and technical safeguards implemented and maintained in accordance with data protection law and relevant standards to protect personal data.
2. Accountability
	1. CTE must implement appropriate technical and organisational measures to ensure compliance with data protection principles (set out in 4.2 above). CTE is responsible for, and must be able to demonstrate compliance with the data protection principles.
	2. CTE must have adequate resources and controls in place to ensure and to document data protection law compliance including:
		1. assigning data protection compliance to the General Secretary;
		2. implementing data protection by design and default when processing personal data to ensure compliance with applicable data protection laws (see section 12 below);
		3. completing Data Protection Impact Assessments (DPIAs) to identify and reduce risks of a data processing activity, where processing presents a high risk to the rights and freedoms of individuals. DPIAs should be conducted for all major system or business change programs involving the processing of personal data particularly those involving new initiatives or technology (see section 12 below);
		4. integrating data protection into internal documents, policies and procedures including this Data Protection Policy;
		5. regularly training staff on applicable data protection law, this Data Protection Policy, related policies, guidelines and data protection matters including, for example, individual rights, consent, legal basis, DPIAs and personal data breaches; and
		6. 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.
3. Privacy By Design and Data Protection Impact Assessment (DPIA)
	1. CTE is required to implement privacy by design when processing personal data by implementing appropriate technical and organisational measures in an effective manner, to ensure compliance with data privacy principles.
	2. CTE must assess what privacy by design measures can be implemented on all programs/systems/processes that process personal data by taking into account the following:
		1. the state of the art (i.e. the highest level of general development, as of a device, procedure, process or technique achieved at the particular time);
		2. the cost of implementation;
		3. the nature, scope, context and purposes of processing; and
		4. the risks of varying likelihood and severity for rights and freedoms of individuals posed by the processing.
	3. CTE mustconduct DPIAs in respect of processing which is considered to be high risk (for example where processing involves special category personal data on a large scale).
	4. Staff should contact the General Secretary and conduct a DPIA when implementing major system or business change programs involving the processing of personal data including:
		1. use of new technologies (programs, systems or processes), or changing technologies (programs, systems or processes);
		2. automated processing including profiling and automated decision making;
		3. large scale processing of special category data; and
		4. large scale, systematic monitoring of a publicly accessible area (e.g. under CCTV).
	5. A DPIA must include:
		1. a description of the processing, its purposes and the data controller's legitimate interests if appropriate;
		2. an assessment of the necessity and proportionality of the processing in relation to its purpose;
		3. an assessment of the risk to individuals; and
		4. the risk mitigation measures in place and demonstration of compliance.
4. Consent
	1. CTE must ensure personal data is processed on the basis of one or more of the lawful bases set out in 5.2 above, one of which is consent.
	2. In order for an individual to validly consent to the processing of their personal data, that consent must be freely given, specific, informed and be an unambiguous indication of the individual’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.
	3. Consent requires *affirmative* action so silence, pre-ticked boxes or inactivity are not sufficient.
	4. If consent is given in a document which deals with other matters, then the consent must be kept separate from those other matters.
	5. Individuals 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 CTE intends to process personal data for a different and incompatible purpose which was not disclosed when the individual first consented.
	6. Consent should not be relied upon as the legal basis for processing, if another more appropriate legal basis applies.
	7. Consent should not usually be relied upon where there is an imbalance in the relationship between the individual and CTE for example in the context of an employer/employee relationship.
	8. Explicit consent may be required for:
		1. Processing special category personal data which includes personal data revealing an individual’s religious or similar beliefs (see sections 5.4 - 5.9 above). Staff should contact the General Secretary to determine the most appropriate legal basis for processing special category data in other instances.
		2. Automated decision-making; and
		3. Cross border data transfers.
	9. Explicit consent requires a very clear and specific statement of consent from the individual and the individual should be provided with detailed information in relation to the specific purpose for which explicit consent it being sought.
	10. Staff should keep records of all consents so that CTE can demonstrate compliance with consent requirements.
5. Limitations on transfers of data
	1. Data protection law restricts data transfers to countries outside the European Economic Area (‘EEA’) in order to ensure that the level of data protection afforded to individuals is not undermined. Personal data is transferred from the originating country across borders when it is transmitted, sent, viewed or accessed in a different country.
	2. CTE may only transfer personal data outside the EEA if one of the following conditions applies:
		1. the European Commission has issued a decision confirming that the country to which the personal data is transferred ensures an adequate level of protection for the individuals’ rights and freedoms (an ‘adequacy decision’);
		2. appropriate safeguards are in place such as binding corporate rules (which are standard contractual clauses approved by the European Commission), an approved code of conduct or a certification mechanism;
		3. the individual has provided explicit consent to the proposed transfer after being informed of any potential risks; or
		4. the transfer is necessary for one of the other reasons set out under data protection law including the performance of a contract between CTE and the individual, reasons of public interest, to establish, exercise or defend legal claims or to protect the vital interests of the individual where the individual is physically or legally incapable of giving consent and, in some limited cases, for CTE’s legitimate interest.
	3. Staff should contact the General Secretary before transferring personal data outside the EEA to ensure one of the conditions outlined above is satisfied.
6. Sharing Personal Data
	1. CTE will not share personal data with third parties unless appropriate safeguards and contractual arrangements have been put in place.
	2. Staff may only share the personal data held by CTE with another employee, representative or individual within CTE if the recipient has a job-related need to know the information.
	3. Staff may only share special category personal data about members, former members and individuals in regular contact with CTE if sharing that special category data is in the course of the legitimate activities of CTE.
	4. Where CTE uses external organisations to process personal data on its behalf, appropriate security arrangements will be implemented in contracts with those organisations to safeguard the security of personal data.
	5. Staff should consult the General Secretary to discuss the necessary steps to ensure compliance when setting up any new agreement or altering any existing agreement.
7. Individuals’ rights and requests
	1. Individuals have rights when it comes to how CTE handles their personal data. These include rights to:
		1. receive certain information about CTE’s processing activities in a Privacy Notice (see section 5.10 above);
		2. request access to their personal data that CTE holds (via a subject access request) (access);
		3. ask CTE to erase personal data if it is no longer necessary in relation to the purposes for which it was collected or processed (erasure);
		4. rectify inaccurate data or to complete incomplete data (rectification);
		5. restrict processing in specific circumstances (restriction);
		6. 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 (data portability);
		7. withdraw consent to processing at any time where that is the legal basis for processing;
		8. prevent CTE’s use of their personal data for direct marketing purposes;
		9. challenge the legal basis on which their personal data is being processed;
		10. request a copy of an agreement under which personal data is transferred outside of the EEA;
		11. prevent processing that is likely to cause damage or distress to the individual;
		12. be notified of a personal data breach which is likely to result in high risk to their rights and freedoms; and
		13. make a complaint to the supervisory authority.
	2. Staff must immediately inform the General Secretary of any request received in relation to the rights outlined above in accordance with CTE’s Subject Access Request Policy and Individual Rights Policy. This is particularly important because CTE must respond to a valid request within the legally prescribed time limits (under GDPR in the majority of circumstances this is 1 month from the day the request is received).
8. Informing members of CTE and its Member churches and Bodies in Association
	1. CTE is subject to certain rules and privacy laws when informing members and other individuals about certain CTE activities, events, fundraising drives, etc.
	2. Prior consent is required for publicising events through electronic communication (for example, by email, text or automated calls).
	3. The right to object to being kept informed (i.e., opt-out or unsubscribe) must be explicitly offered to the individual in an intelligible manner so that it is clearly distinguishable from other information, when their personal data is collected and in every subsequent communication.
	4. An individual's objection to being kept informed must be promptly honoured. If a member or other individual opts out 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.
9. Reporting a Personal Data Breach
	1. Data protection law requires CTE to notify personal data breaches to the relevant supervisory authority (e.g., the Information Commissioner’s Office) and individual data subjects, in certain circumstances.
	2. Staff should be aware that a personal data breach is any act or omission that compromises the security, confidentiality, integrity or availability of personal data or the physical, technical, administrative or organisational safeguards that CTE 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.
	3. If staff know or suspect that a personal data breach has occurred, they should not attempt to investigate the matter themselves. Staff should immediately contact the General Secretary in the event of a personal data breach.
	4. Staff should ensure that they preserve all evidence relating to the potential personal data breach.
10. Consequences of failing to comply
	1. CTE takes compliance with this Data Protection Policy very seriously. Failure to comply puts both staff and CTE at risk. The importance of this data protection policy means that failure to comply with any requirement may lead to disciplinary action, which may result in dismissal.
11. Review of this Policy
	1. CTE reserves the right to change this Data Protection Policy at any time without notice. Staff should ensure that have the latest copy of this Data Protection Policy.
12. Acknowledgement of receipt and review
	1. I, [EMPLOYEE NAME], acknowledge that on [DATE], I received and read a copy of CTE's [Data Protection Policy][, dated [EDITION DATE]] and understand that I am responsible for knowing and abiding by its terms. [I understand that the information in this Data Protection Policy is intended to help staff work together effectively on assigned job responsibilities and assist in the use and protection of personal data.] This Data Protection Policy does not set terms or conditions of employment or form part of an employment contract.

Signed ……………………………………………………….

Printed Name ……………………………………………….

Date ………………………………………………………….

Approved by Board of Trustees of Churches Together in England

Signed

Dated

Reference Minute

**APPENDIX 1**

**Disposal & Retention Checklist**

When determining how long specific categories of personal information should be retained, CTE must, in accordance with the data protection principles, assess:

* The nature of the personal information held and CTE’s reasons for processing it and whether these remain valid;
* The cost, risks and potential liabilities associated with retaining the data;
* The ease or difficulty of making sure that the personal information remains accurate and up to date.

The following questions and guidance should be considered prior to the disposal of any personal information.

|  |  |  |
| --- | --- | --- |
| **1.** | **What is the personal information used for and is it still used for the reason it was collected?**Information that continues to be necessary for the reason it was initially collected can lawfully be retained as long as that reason still applies. If, however, that information is no longer necessary for the reason it was collected, and CTE has no other legal basis for retaining the personal information, it should be disposed of appropriately in accordance with this Policy.Personal data should not be kept "just in case", or if there is only a small possibility that it will be used.NB. Consider whether all the personal information is necessary, or whether only some of the personal information needs to be retained. |  |
| **2.** | **Are there legal [or regulatory] requirements that mandate the retention or deletion of the data?**CTE is permitted to retain personal data to comply with a legal requirement (for example, tax, auditing, or health and safety) [or a requirement set out in professional guidelines to which we are subject]. |  |
| **3.** | **Are there any industry practices regarding the retention or deletion of the data in place?**Specific sector requirements and agreed practices to retain personal data may be in place (for example, credit reference agencies are generally permitted to keep consumer credit data for six years). |  |
| **4.** | **Is retention required for evidence?**CTE may need to keep personal information in relation to any potential or ongoing legal proceedings until the threat of proceedings has passed, or ongoing legal proceedings have concluded.The limitation period for commencing litigation should also be a key consideration. The main time limits that may apply to CTE are:Contract or tort claims (such as negligence) other than personal injury – 6 years from the date on which the cause of action occurred;Personal injury claims – 3 years from the date on which the cause of action occurred;Claims relating to employment such as unfair dismissal or discrimination – 3 months from the date dismissal or the alleged unlawful act. |  |
| **5.** | **Does the personal information need to be retained for historical, statistical or research purposes?** Processing for these purposes can continue for as long as is needed, provided appropriate technical and organisational measures are put in place in relation to this information, particularly to ensure that only the minimum amount of information necessary is retained. |  |

**APPENDIX 2**

**RETENTION SCHEDULE**

1. The Retention Schedule sets out the period CTE recommends for each category of personal information processed by us. The retention period sets out in the Retention Schedule applies to all personal information in that category by default, and should be adhered to wherever possible.
2. CTE recognises that there may be exceptional circumstances which require personal information to be kept for a longer period than is designated under the Retention Schedule. If particular personal information requires a different retention period than that recommended under the Retention Schedule then the Head of Legal should be contacted to discuss and, if appropriate approve any specific retention requirements.
3. In the event that a category of personal information is not covered by the provisions of the Retention Schedule then the Disposal & Retention Checklist should be used to determine whether the personal information needs to be retained, and the appropriate period of retention.
4. In any instance where specific retention periods are agreed (either because they depart from those contained in the Retention Schedule or relate to a category of personal information not contained in the Retention Schedule) that retention period should be:
	* 1. Documented; and in the case of a departure from the Retention Schedule
		2. The reasons for the departure noted; and
		3. Any affected data subjects should be notified.
5. The retention periods set out in the retention schedule apply to all formats of documents, i.e. paper and electronic, unless specifically stated otherwise.
6. In circumstances where the retention period of a document containing personal information has expired, a review should be carried out prior to a decision being made to dispose of it, in accordance with the Disposal & Retention Checklist.
7. The Operations Manager will be responsible for ensuring that the Retention Schedule is kept up to date, to reflect changing organisational needs, new legislation and changing perceptions of risk management.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **DEPARTMENT** | **CATEGORY OF PERSONAL DATA/INFORMATION** | **MEDIA** | **RETENTION PERIOD** | **FACTORS INFORMING RETENTION PERIOD** |
| *HUMAN RESOURCES* | *Records of recruitment exercises including;** *Applicants CVs and accompanying documentation;*
* *Correspondence\*; and*
* *Interview notes*
 | *Paper and electronic* | *Review 6 months from end of the recruitment exercise* | *Statutory limitation period for contractual/employment tribunal claim* |
| *DBS Certificates* | *Paper and electronic* | *Until offer of employment is made, thereafter retain only fact that DBS check has been carried out and the date* | *Once decision is made to recruit, the DBS check is deemed satisfactory and no need to retain further* |
| ***Employee files****Including:**Contracts of employment**Payroll records**Date of any DBS check**disciplinary record,* *grievances,* *absence record,**leave record,**personal injuries at work,**references,**work permits**termination agreements**workplace correspondence\*, etc.* | *Paper and electronic* | *7 years after employment has ended* | *Statutory limitation period, for contractual/employment tribunal claim;**Regulatory or legal requirements* |
| *Basic employee record: start date, end date, reason for leaving, job roles.* |  | *20 years after employment has ended.* | *Provision of references, statistical historical purposes.* |
| *Pension administration documentation* |  | *Indefinitely* | *In accordance with pension scheme requirements.* |
| *Occupational Health records including:**Health questionnaire**Adjustments to workplace**Restrictions**Recommendations* |  | *7 years after employment has ended* | *Statutory limitation period, for contractual/employment tribunal claim;**Regulatory or legal requirements* |
| *ADMINISTRATIVE DOCUMENTATION* | *Internal meeting minutes**Correspondence\***Funding applications* |  | *3 years after last action* |  |
|  *MEMBER INFORMATION* | *Member enquiries and client documentation* | *Paper and electronic* | *6 years after member relationship has ended* | *Statutory limitation period, for contractual claim;* |
| *Direct marketing contact information* | *Paper and electronic*  | *Indefinitely or until the member opts-out* |  |
| *Complaints* | *Paper and electronic*  | *6 years after last action* |  |
| *EMAILS* | *All email correspondence* | *Electronic* | *This period will likely depend upon the storage capacity and may result in indefinite retention, or for example retention for a period of 99 years* |  |
| *AUDIO/VISUAL* | *CCTV* | *Electronic* | *This period will likely depend upon the storage capacity* |  |

\*Any email correspondence will be retained in accordance with the specific retention period for emails specified in the Retention Schedule.