GDPR Data Protection Policy

Contents

1. Policy Control

Version	Description	Date
1.01	Draft GDPR policy	03/18
Tom B - Head of Business Support & Development		
v.2	Approved by Board	04/18

1.1. Related policies

Version	Description	Date of Update
1.2	Privacy Policy	April 2018
1.1	Retention and Disposal Policy	April 2018
1.3	ICT usage policy	Oct 2016
1.2	Communications Policy	Feb 2017

2. Introduction

CFW provides a broad range of service to individuals and organisations. As a result CFW needs to process personal and (in certain circumstances) personally sensitive data, also know as “special category data”, about its employees, trustees, volunteers, members, clients and the public to enable it to meet its legal requirements and responsibilities.
To comply with the Data Protection Legislation in England and Wales (including GDPR that will replace a prior European Union privacy directive known as Directive 95/46/EC). personal information processed must be collected and used lawfully, stored in a secure manner, not stored longer than is strictly necessary and not used for any other purpose other than for which it was provided.

These changes have implications for many of the aspects of the Company’s Operations, Finance, IT, HR, Communications, etc. They also impact on how we deal with customers and external organisations. The regulations cover in specific detail our requirements to ensure organisation wide: Awareness, Information Held, Communicating Privacy Information, Individuals’ Rights, Subject Access Request, Legal Basis for Processing Personal data, Data Breaches, Data Protection Impact Assessments, Data Protection Officers, and International Implications.

This policy sets out CFW’s approach to meeting the new requirements and, more importantly, ensure that all personal information is held securely and with the informed

consent of the data subject where we have no lawful basis to process personal information otherwise.

The following sections detail the Company's approach to each aspect of the new General Data Protection Regulations. If you have any questions, please speak to your Line Manager in the first instance.

In summary requirements under Data Protection Legislation state CFW must:

- maintain up to date records of processing activities under our responsibility and make appropriate records available to the data subject on request.

- Process the Personal Data only in accordance with the consent for which it was provided [which may be specific instructions or instructions of a general nature as otherwise notified by the terms of service provided] and for no other purpose;

- Process the Personal Data only to the extent, and in such manner, as is necessary for the provision of the service requested or as is required by Law or any Regulatory Body;

- implement appropriate technical and organisational measures to protect the Personal Data against a breach of security caused by unauthorised or unlawful processing and against accidental or unlawful destruction, loss, damage, alteration or unauthorised disclosure of or access to the Personal Data. These measures shall be appropriate to the risk of harm which might result from any such breach of security having regard to the nature of the Personal Data which is to be protected as shall be required by Article 32 -36 GDPR when this becomes applicable.

- Take adequate measures to ensure the reliability of any third party supplier Personnel who are authorised to access the Personal Data;

- ensure that third party supplier Personnel without appropriate authority do not have access to the Personal Data.

- obtain specific opt-in consent from the data subject in order to transfer the Personal Data to any Subcontractors or affiliates for the provision of the Services and oblige by way of contract or other legal authority any Subcontractors or affiliates to comply with the same data protection obligations as those set out in data protection legislation.

- Inform the subject where Personal Data is stored outside of the European Economic Area (EEA).

- ensure that all representatives required to access the Personal Data are informed of the confidential nature of the Personal Data and comply with the obligations set out in this policy;

- ensure that all our representatives with access to the personal data receive an adequate level of training in data protection

- Ensure that our representatives do not publish, disclose or divulge any of the Personal Data to any third party unless required to do so under Data Protection Legislation or to meet our legal obligations unless explicit consent has been obtained by the data subject.

All staff and volunteers who process or use any Personal Information must ensure that they follow these principles at all times. In order to ensure that this happens, the company has adopted this Data Protection Policy.

Any member of staff, trustee or volunteer, who considers that this policy has not been followed in respect of personal data about him/herself or a customer of CFW should raise the matter with the Designated Data Controller (Tim Houghton).

If the matter is not resolved, it should be raised as a formal grievance (if relating to the employee) or through the company's Whistleblowing Policy if it relates to a customer.

3. Conditions for processing personal data

In addition to the principles set out above Under Data Protection legislation CFW is subject to additional accountability and transparency requirements (in line with Articles 5(2) and 24 of the GDPR), and in each instance demonstrate adequate due process to evidence:

☐ We have reviewed the purposes of our processing activities, and selected the most appropriate lawful basis (or bases) for each activity.

☐ We have checked that the processing is necessary for the relevant purpose, and are satisfied that there is no other reasonable way to achieve that purpose.

☐ We have documented our decision on which lawful basis applies to help us demonstrate compliance.

☐ We have included information about both the purposes ("fairness") of the processing and the lawful basis for the processing in our privacy notice.

☐ Where we process special category data (personally sensitive data), we have also identified a condition for processing special category data, and have documented this.

3.1 Lawful basis for processing personal data

CFW must satisfy itself we have identified the lawful basis for processing personal information, set out in Article 6 of the GDPR. We are required to clearly document our lawful basis for processing across each of our activities. The six lawful bases for

processing are:

(a) Consent: the individual has given clear consent for CFW to process their personal data for a specific purpose.

(b) Contract: the processing is necessary under contract with the individual, or because they have asked CFW to take specific steps before entering into a contract.

(c) Legal obligation: the processing is necessary to comply with the law (not including contractual obligations).

(d) Vital interests: the processing is necessary to protect someone's life.

(e) Public task: the processing is necessary to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

(f) Legitimate interests: the processing is necessary for legitimate interests of the company or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

CFW must as part of our privacy statements for each service inform people upfront about the lawful basis for processing their personal data. We must communicate this information to individuals by 25 May 2018, and ensure that we include it in all future privacy notices. For most activities undertaken by CFW the lawful basis for processing personal data is equivalent to those used under DPA (1998).

3.2 Processing Special Category Data

Special category data is broadly similar to the concept of sensitive personal data under the 1998 Act.

Special category data is more sensitive, and so needs more protection meeting the "secure by design" principle under Data protection legislation. For example, information about an individual's:

- race;
- ethnic origin;
- politics;
- religion;
- trade union membership;
- genetics;
- biometrics (where used for ID purposes);
- health;
- sex life; or
- sexual orientation.

This list is not exhaustive and also includes other protected characteristics as outlined in Equalities legislation (2010).

In specific instances CFW is required to process special category data in order to meet our legal duties and responsibilities. In such instances CFW must satisfy itself that we have identified both a lawful basis under Article 6 and a separate condition for processing special category data under Article 9. These do not have to be linked.

points of Article 9(2)—
(a) point (b) (employment, social security and social protection);
(b) point (g) (substantial public interest);
(c) point (h) (health and social care);
(d) point (i) (public health);
(e) point (j) (archiving, research and statistics).

(Genral Data Protection Bill Clauses 9, 10 Accessed at:
https://publications.parliament.uk/pa/bills/lbill/2017-2019/0074/18074.pdf)

CFW must in the case for processing special category data inform the data subject of the lawful basis under which we process their data including the condition for processing under Article 9 of the GDPR (or any successor legislation).

4. Data Subjects Rights

Central to Data Protection legislation are the rights of data subjects. These enhanced rights reflect the primacy of the basic human right to privacy. Rights of data subjects include:

Right to be informed
Right of access
Right to rectification
Right to erasure
Right to restrict processing
Right to data portability
Right to object
Rights related to automated decision making including profiling

4.1 Privacy Statement and consents

The Company will issue an individual a Privacy Statement specific to each service provided to the individual by the company. This will detail all the types of personal information which the Company holds and processes, its purposes, how it is processed, why and the policy/security provisions enacted by the company to ensure it's safe keeping.

The Statement will also detail how an individual can have access to their information should they wish to. Individuals have the right to amend inaccuracies, or delete any information held under their right to erasure as outlined above.

In certain circumstances CFW can refuse to comply with a request for erasure "right to be forgotten" where the personal data is processed for the following express reasons:

- to exercise the right of freedom of expression and information;
- to comply with a legal obligation for the performance of a public interest task or exercise of official authority.
- for public health purposes in the public interest;
- archiving purposes in the public interest, scientific research historical research or statistical purposes; or
- the exercise or defence of legal claims.

Guidelines produced by the ICO (included below) outline the information to be supplied to to the individual as part of obtaining consent. These are to be included in the terms and conditions of service and accompanying privacy policy specific to each activity that requires the company to process personal data.

What information must be supplied?	**Data obtained directly from data subject**	**Data not obtained directly from data subject**
Identity and contact details of the controller (and where applicable, the controller's representative) and the data protection officer	✓	✓
Purpose of the processing and the lawful basis for the processing	✓	✓
The legitimate interests of the controller or third party, where applicable	✓	✓
Categories of personal data		✓
Any recipient or categories of recipients of the personal data	✓	✓
Details of transfers to third country and safeguards	✓	✓
Retention period or criteria used to determine the retention period	✓	✓
The existence of each of data subject's rights	✓	✓
The right to withdraw consent at any time, where relevant	✓	✓
The right to lodge a complaint with a supervisory authority	✓	✓
The source the personal data originates from and whether it came from publicly accessible sources		✓
Whether the provision of personal data is part of a statutory or contractual requirement or obligation and possible consequences of failing to provide the personal data	✓	
The existence of automated decision making, including profiling and information about how decisions are made, the significance and the consequences	✓	✓

When should information be provided?	At the time the data are obtained.	Within a reasonable period of having obtained the data (within one month)
		If the data is used to communicate with the individual, at the latest, when the first communication takes place; or
		If disclosure to another recipient is envisaged, at the latest, before the data are disclosed.

(https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-be-informed/ Accessed on 12/03/2018)

The right to be informed encompasses our obligation to provide 'fair processing information', typically through a privacy notice.

The information supplied to the subject about the processing of their personal data must be:

- concise, transparent, intelligible and easily accessible;
- written in clear and plain language, particularly if addressed to a child; and
- free of charge.

5. Roles and Responsibilities

CFW as a Charity and a Company Limited by Guarantee is the Data Controller under Data Protection legislation, and the organisation is ultimately responsible for ensuring compliance with the GDPR (or subsequent legislation).

5.1 Third party Contracts

Where CFW uses the services of other third parties who are required to act as data processors, CFW will enter into written contract with the the third party setting out the roles and responsibilities of both parties.

A contract will only be entered into with a data processor where a third party can demonstrate 'sufficient guarantees' that the requirements of the GDPR will be met and the rights of data subjects protected and where the terms of the contract require Processors to

only act on the documented instructions of the controller.

Our contracts include the following compulsory details:

- the subject matter and duration of the processing;
- the nature and purpose of the processing;
- the type of personal data and categories of data subject; and
- the obligations and rights of the controller.

5.2 Data Protection Officer and Board of Directors

The designated Data Protection Officer (DPO) within CFW is the Chief Executive, Tim Houghton.

The DPO reports directly to the Board who is ultimately responsible for the activities of the company.

The DPO's responsibilities are defined in Article 39 of GDPR:

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

5.3 Managers, employees and other authorised representatives

Day to day management and implementation of the company's Data Protection processes and procedures may be delegated by the DPO to the relevant departmental Head of Service.

Departmental Heads of Service work with the DPO to ensure that service specific operational processes adequately reflect CFW policy and relevant legislative requirements

All employees and representatives of the company, including third parties and volunteers, who process or use any Personal Information are responsible for ensuring that:

- Any Personal Information which process is kept securely; and
- Personal Information is not disclosed either orally, electronically, in writing or by any other means to an unauthorised party.

Staff and volunteers should note that unauthorised disclosure will likely be a disciplinary matter, and may be considered gross misconduct.

Any enquiries about any aspect of the Company's data protection should be directed to the Data Processing Officer or the appropriate Head of Service, including general queries, specific personal data questions.Subject Access Requests and real or potential breaches of

data or data protection requirements should be made to the DPO (cf. Investigation and SAR below).

6. Security

Under Data Protection Legislation the Company is required to implement technical and organisational measures to evidence of how we have considered and integrated data protection into processing activities. The principal of secure by design includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage. It requires that appropriate technical or organisational measures are used.

6.1 Regular reviews

The Data Protection Officer will undertake annual reviews of the data protection policies and procedures and provide a report to the Board on the current situation with any risks identified and remedial action required through the company's risk register reporting process.

6.2 Privacy/Data impact assessments (PIA)

Simple Privacy or Data impact assessments will be conducted by the appropriate Departmental Head of Service under the oversight of the DPO at the beginning or in the early stages of new projects or services to identify the most effective way to comply with their data protection obligations and meet individuals' privacy rights.

The purpose of a PIA is to ensure that privacy risks are minimised while allowing the aims of the project to be met. Risks can be identified and addressed at an early stage by analysing how the proposed uses of personal information and technology will work in practice. Some of the ways risks can arise are through personal information being: inaccurate, insufficient or out of date; excessive or irrelevant; kept for too long; disclosed to those who the person it is about does not want to have it; used in ways that are unacceptable to or unexpected by the person it is about; or not kept securely.

6.3 Training of staff

All staff will undertake training and/or briefing sessions detailing the Company's and their personal responsibilities under the data protection regulations. This will be covered in the induction training for new starters including for volunteers and company Directors.

6.4 Electronic data

CFW use a range of third party applications and services (Infrastructure as a Service e.g. Google Drive and Software as a Service products e.g. Mailchimp, Sage, Community Access, Paloma, Co-Impact etc.) for the processing of personal data. In each case CFW enter into contract(s) with each supplier detailing the Terms of Service and roles and responsibilities of both parties under data protection legislation. CFW must satisfy itself that that the supplier meets the requirements set out in S.5.1 above.

All employees are subject to CFWs Information and Communication Technologies Usage Policy accessible here, also via the Intranet or in each office location. CFW ICT usage policy setouts out employee roles and responsibilities when processing data electronically.

For each Line of Business application CFW has appropriate documentation to evidence appropriate technical and organisational measures to demonstrate that personal data is secure. Data Processor Agreements are in place with all third party suppliers for each Line of Business Application.

6.5 Paper/hard copy records

CFW seeks to minimise the use of print copy where appropriate. It is recognised that in many instances hard copy records are required for administration processes. Where hard copy records are kept it is the responsibility of the relevant HoS with the DPO to:

- Under take a Privacy Impact Assessment (cf. 6.2 above)
- Identify and implement appropriate technical and organisational measure to ensure the safekeeping of personal and special category data.
- Document operational processes for the effective administration and safekeeping of hard copy records.
- Review the process to ensure effectiveness.

Personal Data must only be kept as long as is strictly necessary for the processing activity. As part of the PIA the lawful basis for processing data will be identified and any other conditions necessary for the processing of special category data (cf. S3 above). For specific guidance on how long different type of data can be held refer to the Retention and Disposal policy set out below.

Archiving and secure disposal services are provided to CFW from Hampshire based firm Box-it. The lead contact within CFW responsible for the management hard copy archive and disposal services is Jean Field (Finance Officer) in the Finance Department.

6.6 Telephone Conversations and Meetings

- If personal information is collected by telephone, callers should be advised what that information will be used for and their rights under Data Protection Legislation.

- Personal or confidential information should preferably not be discussed in public areas of CFW's work premises or within open-plan office areas. Wherever possible, visitors should be escorted to a private interview room or office and not be permitted to wander about the premises on their own. If possible, visitors should subsequently be escorted out of the premises when the meeting is over.

All staff should be aware of the difficulties of ensuring confidentiality in an open plan area and respect the confidential nature of any information inadvertently overheard.

Any notes taken during or after an interview should be of relevance and appropriate. It is recommended that such notes are subsequently securely filed in a legible and coherent

manner and that informal notes are retained for only a short period (no longer than 12 weeks), in a secure place, before being shredded or securely deleted.

7. Investigation and reporting

Data Protection Legislation places a duty on all organisations to report certain types of personal data breach (Recital 87 of the GDPR). CFW are required to ensure robust processes for breach detection, investigation and internal reporting procedures. This will facilitate decision-making about whether there is a requirement to notify the relevant supervisory authority and the affected individuals. Where this is the case inform the ICO or relevant authority within 72 hours of becoming aware.

The DPO is responsible for conducting any data breach investigations, recording and reporting. The DPO may deputise these responsibilities to the appropriate Head of Service but will retain oversight of assuring the investigation and reporting process. As part of the Investigation and reporting process the DPO will ensure:

- assessment of the likely risk of harm to individuals resulting from a breach.
- Contact the relevant supervisory authority for respective processing activities.
- Notify the ICO of the breach (subject to reporting requirement) within 72 hours of becoming aware of it, even if all the details are not fully known.
- Collate relevant information in relation to the suspected breach to supply to the ICO.
- Inform affected individuals about the breach when it is likely to result in a high risk to their rights and freedoms without undue delay.
- Provide to individuals information about a breach, and provide advice to help them protect themselves from its effects.
- Internally document all breaches, even if they don't need to be reported.

Reportable breaches may include but are not limited to material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned.

8. Subject Access Request (SAR)

Data Protection legislation assures the rights of individuals to access their personal data; so that they are aware of and can verify the lawfulness of the processing (Recital 63).

Under the legislation individuals have the right to obtain:

- confirmation that their data is being processed;
- access to their personal data; and

- other supplementary information – aligned with Data subject rights contained in S.4.1 above (Cf. Article 15 of the GDPR).

CFW will make SARs available free of charge, unless it is deemed unfounded or excessive, or where repeated requests for the same information have been made. In cases where a fee is applied to a SAR this will based on the administrative cost of providing the information.

9. Data Retention and disposal

CFW will keep some types of information for longer than others. Where the legal basis for processing data is consent; information will be kept for 'no longer than is necessary' this is considered to be up to two years after the subject last accessed CFW services, unless other bodies, such as funders, require CFW to keep the information longer under contract or where another lawful basis for processing information is used e.g. HMRC reporting purposes. The lawful basis for processing is identified for each activity and is documented. In each instance personal and special category data is minimised or anonymised wherever reasonable.

The following is a list of data subjects. A data subject is an individual about whom personal data is held. The following data subjects are permitted:

a) Employees and Volunteers

b) customers

c) members or supporters

d) third party suppliers

e) representatives from partner agencies

The schedule below shows periods for the retention of the various types data processing activity including personal and or sensitive (special category) information records held by CFW:

The schedule below shows recommended periods for the retention of the various types of information:

Type	**Item**	**Description**	D**isposal (maximum period)**
1. Client			

/customer records	1.1	Enquiries	2 years from last contact
	1.2	Complaint Investigations	6 years
	1.3	Aggregated statistical reports	3 years
	1.4	Case files or Order history	3 years *(unless required for longer under contract - in which case to be communicated via the specific terms of service)*
	1.5	Payment history (cf.Financial records)	7 years
	1.6	FOI/SAR requests inc. associated correspondence	2 years if accepted by the company; otherwise 6 years
	1.7	Register of Complaints	5 years
	1.8	General Correspondence	2 years
	1.9	Safeguarding Concern Form and Associated investigations/ reports.	Permanently

2.0 Project records	2.1	contract monitoring Reports	3 years
	2.2	project specific policies and operating procedures	2 years from conclusion from area of work
	2.3	Impact Assessments (Privacy and Equality)	3 years
	2.4	Contacts inc. MoU and SLA or Grant Agreements	7 years
3.0 Workforce & personnel	3.1	Recruitment and selection material	6 months after the decision
	3.2	References	7 years
	3.3	employment contracts	7 years
	3.4	Leave and absence records	2 years
	3.5	Performance records such as training, appraisal and disciplinary	2 years
	3.6	Employee's home address, Next of Kin details	six months from ending employment
	3.7	Payroll records and relevant supporting documents	7 years
	3.8	Whistleblowing	Permanently
	3.9	DBS - registration number and date of issue only	3 years from issue
4.0 Financial Records	4.1	Budgets and management accounts	3 years from Financial Year End

	4.2	Annual accounts	Permanently
	4.3	External Audit reports	Permanently
	4.4	Bank/ Credit statements	7 years
	4.5	VAT returns	7 years
	4.6	Ledger	Permanently
	4.7	Invoices - Capital, revenue, rate and rent invoices and supporting estimates.	7 years
	4.8	Employee expenses claims	3 years
	4.9	Debtors' records	7 years
5.0 Governance and Legal	5.1	Accident books and accident records	3 years from last entry
	5.2	Board meeting minutes	Permanently
	5.3	Memorandum of Understanding (MOU)	Permanently
	5.4	Trust Deed	12 years
	5.6	Supplier Contracts	7 years from end of contract
	5.7	litigation and formal legal advice	Permanently