Covid-19 Bereaved Families for Justice

Data Protection Policy

Version	2.0
Release Date	April 2024
Review Date	April 2026

Table of Contents

Introduction

Covid-19 Bereaved Families For Justice has a responsibility to follow the rules of the Data Protection Act 2018 (the Act) and the UK General Data Protection Regulation (UK GDPR). This guidance will help staff and volunteers to comply with data protection requirements set out in UK law. For any clarification needed contact the Data Protection Lead at hello@covidfamiliesforjustice.org with FAO: Data Protection Lead in the subject, who can also organise any training needed in order to remain compliant.

Policy Statement

This Policy will be reviewed annually or when required, but may also be reviewed at times when the way we collect, store and process the data changes. Covid-19 Bereaved Families For Justice is a Data Controller in accordance with the UK GDPR and must perform a Data Protection Impact Assessment (DPIA) whenever a new processing operation — either a process or processing technology — is proposed. The DPIA, at a minimum, must include the following:

- A description of the new processing operation, its purpose, and necessity relative to the stated purpose.
- An assessment of the potential risks to the rights and freedoms of Data Subjects.
- A description of proposed measures to mitigate risks, including safeguards and security measures.

Data Protection Terms and Definitions

Data protection law applies to how we process people's personal information. The key terms that we need to understand are:

Data Controller: Covid-19 Bereaved Families For Justice Group is a controller wherever it decides what personal information it collects, about whom, and how it will be used.

Data processor: This is a third-party that is used to process personal information on behalf of a controller, usually under a contract. A data processor must only ever act on the written instructions of the controller and does not own or control the personal data.

Principles: These are the rules that we must follow when processing personal information. Under the principles we must be transparent about our use of personal data, and we must be able to demonstrate our accountability under the law.

Processing: This is what we do with personal information. It includes how we collect, record, store, share and use personal information.

Personal data: This includes any information relating to an identified or identifiable living person (see 'data subject' below). An identifiable person is one who

> "can be identified, directly or indirectly, by reference to identifiers such as a name, identification number, location data, online identifiers such as IP address, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person." - Article 4.1 of the UK GDPR.

Special category personal data: This is information about a person's health, religion, political opinion, trade union membership, race or ethnic origin, sexuality.

Personal information: This includes personal data and special category personal data.

A **data subject:** This is the person whose personal information is being processed. For example, a person that is a member on our Action Network System or an employee.

A **privacy policy**: This is how we inform people about how their personal information will be used. The Covid-19 Bereaved Families For Justice Groups' privacy policy will be provided on our website.

A **privacy notice:** This is a short notice when we collect personal information from people to inform them how their personal information will be used and to look at our privacy policy for more detail.

Data protection principles

The principles that we adhere to are set out below.

Lawfulness, fairness and transparency

- We only use data legally under a permitted lawful basis.
- We only use data fairly, being clear, open and honest with people whose data we hold.
- We are clear and open with people about how their personal information will be used.
- Include a written or verbal Privacy Notice when collecting personal information. This should describe:
    - who the controller is.
    - the purpose for which the personal information will be used. For example, to share their story as part of a campaign action.
    - if the personal information will be shared with any other organisations.
- We only use personal information in a way that people would reasonably expect.
- We think about the impact of data processing and would not do anything that could have a negative effect on the people whose personal information we are using.
- We obtain the explicit consent of a person if we are collecting their sensitive (special category) personal data.
- Obtain prior consent from people before publishing photographs, personal stories or film footage of them.
- Where processing data is based on consent, we keep a record of a person's consent, including what a person has specifically agreed to and the date that the consent was given.

Purpose limitation and data minimisation

- We only collect only what we need and use it as planned and communicated via the privacy notice.

Accuracy

- We keep our records up to date.
- We achieve this by regularly asking our members for any changes to their details that we store against them.
- We amend relevant electronic and manual records as soon as possible if someone informs us of a change in their information.

Storage limitation and integrity and confidentiality

- We store data securely and confidentially.
- We must have a valid reason for keeping personal information.
- A data controller must document how long it will keep different types of records and personal information for in a Personal Data Retention Policy and Schedule.
- When personal information is no longer required it must be destroyed or disposed of securely.
- Delete emails containing personal information once no longer needed.

Accountability

- We take responsibility for what we do with the data.
- We have Privacy policies and notices to show what we are doing with the data.
- If we need to send an email containing personal information or attach a file which includes personal information to an email, password protect the email or document, and send the password in a separate email or text message.
- Double check that you have attached the correct file before sending an email.
- Double check that the email is addressed to the correct recipient.
- Always use the bcc field (not the cc field) when sending an email to more than one person so that the recipients' email addresses are not visible to each other - unless consent to share email addresses has previously been obtained.
- Delete emails containing personal information when no longer required or move to a secure file archive if still required.
- Take special care when travelling with computers, laptops, tablets, smart phones and paper records containing personal information.
- Do not leave laptops and files unattended and visible in your car.
- Make sure papers or screens containing personal information are not visible to others in meetings, on trains, and even in your own home.
- Do not download documents containing personal information to any storage device that is not encrypted.

People's rights relating to their data

The purpose of the data protection principles is to keep people safe and respect their rights.

People have a right to:

- understand what data organisations have about them and how it is being used
- see that information and get their own copy of it to use however they want
- correct the information if it is wrong
- ask for it to be deleted or limit how it is used
- complain if they don't like things an organisation is doing with their data.

Personal data breach — what to do

Personal data breaches occur when personal information is lost, destroyed or shared without consent, or if someone accesses the personal information or passes it on without consent. This can be deliberate or by accident. It includes sending personal information to the wrong person in an email or electronic devices, such as laptops and telephones containing personal information being lost or stolen. We must act quickly if this occurs.

- If you think there may have been a data protection breach or there has been a near miss, please let the Covid-19 Bereaved Families For Justice Data Lead know immediately by emailing hello@covidfamiliesforjustice.org
- In the breach report you must include factual information; what happened, when, how many people's personal information is affected, and whether any sensitive information was breached e.g. identifiable equalities monitoring data, financial data etc.
- Major data breaches must be reported to the ICO at this Helpline number: 0303 123 1113, or via ICO Website: https://www.ico.ork.uk
- Data controllers must keep a record of all personal data breaches.

Data subject rights

The data protection regulation gives rights to people. The rights that are most relevant to us are:

- **The right to be informed** — we do this by including appropriate privacy notice information when collecting personal information.
- **The right of access** — if asked we must give people a copy of their personal information which we hold.
- **The right to object to processing** — if someone objects to the processing of their personal information we must consider whether we can stop the processing.
- **The right to not receive direct communications** — if a person changes their mind about receiving direct emails and newsletters from us we must stop sending people direct messages.
- **The right to rectification** — we must correct any inaccurate or incomplete personal information when asked.

- **The right to erasure** — we must delete or remove some personal information if we relay on their consent to process it, the data relates to someone under the age of 18 or we have no need to keep it.

Data subject rights — how to respond

The right of access

A person has the right to view their personal information which we hold.

- Individuals have the right to access and receive a copy of their personal data, and other supplementary information.
    - This is commonly referred to as a **subject access request** or 'SAR'.
    - Individuals can make SARs verbally or in writing, including via social media.
- A third party can also make a SAR on behalf of another person.
- Assume that anything you record about a person could be seen by that person.
- Record facts and opinion that you would be able to defend if challenged.
- A person can make a request verbally or in writing to anyone in the organisation.
- When asked we must provide this information within 30 days of it being requested.
- If someone asks to see their personal information, you must complete the template form "Data Subject Request Form" available from the Data Protection Lead and forward it to hello@covidfamiliesforjustice.org without delay.
- The right of access does not extend to include personal information about anyone else unless we have the consent of the other party or parties.
- You may extend the time limit by a further two months if the request is complex or if you receive a number of requests from the individual.
- You should perform a reasonable search for the requested information.
- You should provide the information in an accessible, concise and intelligible format.
- The information should be disclosed securely.
- You can only refuse to provide the information if an exemption or restriction applies, or if the request is manifestly unfounded or excessive.

The right to verify the requestors ID

You need to be satisfied that you know the identity of the requester (or the person the request is made on behalf of). If you are unsure, you can ask for information to verify an individual's identity. The timescale for responding to a SAR does not begin until you have received the requested information. However, you should request ID documents promptly.

The right to object to processing

People have the right to object to Covid-19 Bereaved Families For Justice Group processing their personal information. If someone requests this, explain to them why we process their personal information and any consequences of our not processing it. For example, we would not be able

to send them campaign updates. If the person still objects to the processing, take a note of their contact details and pass it to the Data Protection Lead and forward the request to the Operations and Organisation Development Manager. In some cases an individual cannot object. This will be where the organisation has either a contractual or legal obligation to process the data.

The right to erasure

The right to erasure is also known as 'the right to be forgotten'. People have the right to request the deletion or the removal of their personal information where there is no compelling reason for its continued processing.

- If you have given a person's personal information to someone else, you must contact each recipient of that information and ask them to erase the personal data in question
- If requested, you should also inform the person about the other recipients of their personal information.
- If you have published personal information online, for example on social networks, forums or websites you should also erase the personal information where possible.
- If you receive a right to erasure request, please forward the details to the Data Protection Lead which is the Operations and Organisation Development Manager.

The Lawful Basis

Where personal data is processed to achieve one of the purposes the organisation has identified, a lawful basis must be used prior to any processing activity. This may include but are not limited to:

Consent

We may use the consent of an individual to process their personal data. Where this is the case, it must be informed, freely given and the individual must be able to withdraw such consent. We must ensure that the individual has access to clear privacy information that they may make such an informed choice. If the individual withdraws their consent, we delete all data we were processing.

Legitimate Interest

We may process personal data in the interest of the charity to achieve its objectives. In such cases we must establish that there is a reasonable expectation that the processing activity may occur, that there is no other feasible way to achieve such an objective and that the individual may object to the processing. We may conduct an legitimate interest balancing test in such circumstances.

Contractual obligation

Where we may charge a fee or where we may pay for a service a contractual obligation may be created.

Legal obligation

Where we are bound to process data due to a legal obligation we will process the data according to that obligation and UK data protection law.

Relevant Guidance and Legislation

The Data Protection Act 2018

The UK GDPR

Information Commissioner's Office: https://ico.org.uk/

Other Relevant Policies

To underpin the values and ethos of our organisation, the following policies are also included under our Data Protection umbrella:

Complaints Policy	
Code of Conduct Policy	
Safeguarding Policy	