	**Policy title: Crosscare Data Protection (GDPR) Policy**
	Issue date: OCT 2023

Section 1 – Introduction:

Crosscare has responsibility to maintain the highest standards of confidentiality in the safeguarding of information about its service users, staff members and volunteers.

Information collection is essential to us fulfilling our duties. Data Protection regulation seeks to give people control of their own personal information and so it confers certain obligations on Crosscare in relation to how personal information is collected and used.

Since 25 May 2018 Crosscare operates in line with General Data Protection Regulation (GDPR) and the Data Protection Act 2018.

The aim of this policy is to ensure that each Crosscare staff member has an understanding of the concepts of Data Protection and is aware of their own responsibilities in relation to the organisation's overall compliance with GDPR.

A set of operational procedures for each project and support area of Crosscare accompany this policy. See:

1. Crosscare GDPR Procedures - Food Service, 2023
2. Crosscare GDPR Procedures - Information and Advocacy Services, 2023
3. Crosscare GDPR Procedures - Youth Services, 2023
4. Crosscare GDPR Procedures - Youth Information Services, 2023
5. Crosscare GDPR Procedures - Youth Clubs (affiliated to Crosscare), 2023
6. Crosscare GDPR Procedures - Counselling – (version 1 -Teen Counselling, version 2 - Crosscare Attachment and Mentalization Service, version 3 - Drug and Alcohol Project), 2023
7. Crosscare GDPR Procedures - Homeless Services incl. CLAN, 2023
8. Crosscare GDPR Procedures - Echlin House, 2023
9. Crosscare GDPR Procedures - Aftercare Service, 2023
10. Crosscare GDPR Procedures - Human Resources, 2023
11. Crosscare GDPR Procedures - Volunteers, 2023
12. Crosscare GDPR Procedures - Front-of-house and Administration, 2023
13. Crosscare GDPR Procedures - Accounts, 2023

Section 2 – Definitions:

Data Protection is the safeguarding of the rights of individuals to privacy and integrity in relation to the processing of their personal data.

Data Controller is the natural or legal person (most charities or non-government organisations are data controllers) who, alone or jointly with others, determines the purpose and means of the processing of personal data. In other words, the controller decides what personal data will be processed for and how it will be done.

Data Processor is the legal person such as an individual or a company who processes personal data on behalf of a controller for example, payroll provider, cloud provider, HR provider, if outsourced, etc.

Data processing means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Data Subject is an individual who is the subject of personal data.

In Crosscare **the Data Protection lead** is the individual within an organisation who has responsibility for data protection.

Data means information in any form, which can be processed. Types of data incl.:

- **Personal data** is any information relating to an identified or identifiable natural person ('data subject'). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

- **Special categories of personal data** (this term replaces the term *sensitive personal data*) is personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Section 3 - Data Protection Principles:

The 7 data protection *principles* are the fundamental principles relating to how personal data may be processed. Crosscare must adhere to these principles at all times:

1. Lawful, fair and transparent processing:
2. Purpose limitation
3. Data minimisation
4. Accuracy
5. Storage limitation
6. Integrity and confidentiality
7. Accountability

1. Lawful, fair and transparent processing:

Crosscare will process personal data based on one or more Lawful Processing Conditions ie:

- **Consent**: The Data Subject has clearly and willingly agreed to the processing of their personal data for one or several purposes. An unambiguous, specific indication of the data subject's wishes by a statement or clear affirmative action is needed.
- **Contract**: the processing activity is necessary for the performance of a contract between the Controller and the Data Subject, or necessary at the request of the Data Subject prior to entering into a contract.
- **Legal Obligation**: the processing is necessary for compliance with a legal obligation to which the Controller is subject (e.g. a non-profit organization might be obliged to notify TUSLA where they become aware of allegations of child abuse).
- **Vital Interests**: the processing of the personal data is necessary in order to protect the vital interests of the Data Subject – e.g. in a life and death situation where data is shared on a person's medical situation where the person is not conscious.
- **Public Interest / Official Authority**: the processing is necessary for the performance of a task carried out in the public interest or in the exercise of an official, regulatory or statutory authority, which is vested in the Controller (e.g. where the non-profit organization is acting as an agent for the Department of Social Protection, or the HSE, in providing a service).
- **Legitimate Interest**: the processing is necessary for the purposes of the legitimate interests pursued by the Controller or the Processor, except where these are overridden by the interests or fundamental rights and freedoms of the Data Subject, particularly where he or she is a child.

2. Specified and Lawful Purpose:

Crosscare will process personal data on the basis of one or more specified purposes i.e. data collected for 1 reason (e.g. when a young person applies to join a youth club) cannot be used for a different reason (e.g. to ask that young person's family to contribute to fundraising).

3. Minimisation of processing:

Crosscare will collect personal data limited to what is necessary. A staff member of Crosscare can fulfill this requirement by making sure they only seek and retain the minimum amount of personal data needed for the specified purpose. It should be retained for no longer than is necessary to achieve the purpose or purposes for which it was collected.

4. **Accuracy:**

Crosscare will ensure personal data collected is accurate, and where necessary, kept up to date. A data subject is entitled to have inaccurate personal data concerning themselves rectified without delay, incomplete data concerning themselves completed and to have personal data about them erased. The right to erasure relates to situations where the data subject withdraws consent, objects to the processing or where the personal data has been unlawfully processed, among other reasons. However, the right to erasure is not available where the processing of the relevant personal data is necessary for the establishment, exercise or defence of legal claims, among other reasons.

5. **Storage limitation:**

Crosscare will keep personal data for no longer than is necessary. This requirement places a responsibility on Crosscare to be clear about the length of time each type of data needs to be kept and the reason why the information is being retained. To meet this requirement, Crosscare will ensure that all files are managed, and appropriate retention/disposition schedules are in place within each set of Operational Procedures.

6. **Security and confidentiality:**

Crosscare will process personal data in a manner that ensures 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. The security of personal information is all important, but the key word here is 'appropriate', in that it is more significant in some situations than in others, depending on such matters as confidentiality and sensitivity and the harm which might result from an unauthorised disclosure. High standards of security are, nevertheless, essential for all personal information. The nature of security used may take into account what is available, the cost of implementation and the sensitivity of the data in question.

The minimum standard of security expected of all staff members in Crosscare incl.:

- computer systems password protected
- access to information restricted to authorised staff on a 'need to know' basis
- emails with/without attachments containing personal information are managed very carefully
- information on computer screens and manual files hidden from callers to offices
- back-up procedures in operation for computer held data, including off-site back-up
- waste papers, printouts etc. disposed of carefully by shredding
- employees must locl/log off computers on each occasion when they leave their workstation

- personal security passwords must not be disclosed to any other employees
- premises must be secure when unoccupied.

Project and support area procedures will outline further security requirements in their bespoke procedures documents.

Personal data is used within Crosscare in the normal course of operational functions. Any use or disclosure must be necessary for the purpose(s) or compatible with the purpose(s) for which the data is collected and kept. An employee making a disclosure should consider whether the data subject would be surprised to learn that a particular disclosure is taking place. If the potential answer to this question is yes, then there is a need to question the basis for the disclosure prior to making it.

7. Liability and accountability:

Crosscare will be able at all times to demonstrate how it complies with GDPR. One Senior manager with an overarching responsibility for Data Protection will retain an up-dated folder containing a copy of:

- Crosscare's Data Protection Policy
- Crosscare's Data Protection Procedures (as outlined in **Section 1 – Introduction** of this policy)
- Crosscare Records of Processing Activities Log (RoPA)
- Notes of internal and external Data Protection meetings
- Training Log
- Notes of any other Data Protection matters incl. data breaches etc.

A Crosscare staff member from each project and support area of Crosscare will carry responsibility for GDPR compliance in their project/support area. The assigned senior manager will convene meetings of this group periodically to ensure GDPR compliance throughout Crosscare.

Section 4 – Matters for special attention

Data Subject Rights and Freedoms:

Besides the seven data protection principles above, the GDPR strengthens existing rights and freedoms of the Data Subject and introduces new rights and freedoms.

- Right to be Forgotten: this right to erasure of personal data allows the Data Subject to request from the Controller the deletion of personal data, without undue delay, on particular grounds. In particular, this right is important for Crosscare where they may have collected personal data from a child in the past and where, as an adult, the Data Subject now has a different viewpoint of the risks involved in the processing. In cases of right to erasure, Crosscare is permitted to retain data for which Crosscare has a legitimate or legal purpose to continue processing (for example Crosscare may retain personal data for tax purposes, for HR records or if a legal case is underway). This should be explained to the person seeking the erasure and, when the pension/HR/legal matter no longer requires the data to be retained, it will be deleted.

- Right to Restriction of Processing: in certain circumstances, the Data Subject can request Crosscare to restrict processing either permanently or temporarily. For example, a Data Subject could ask Crosscare not to publish a photograph from a fundraising event showing his or her face until the lawful processing condition for this is clarified.

- Right to Object to Certain Processing: the Data Subject is entitled to object to the processing of their personal data based on his or her situation, preference or state of mind. Where data is processed, for example, for the purpose of direct marketing, consent may be withdrawn at any time and free of charge.

- Right to Data Portability: where a Data Subject is moving their account from one provider to another (or one organisation to another), the Data Subject should be able to receive a copy of his or her personal data in a structured, commonly used, machine readable format.

- Right of Access to Information: The Data Subject has the right of access to their personal data which was collected – this is known as a Subject Access request (SAR). A SAR can be made in writing or verbally. A SAR can be made verbally, Crosscare records the time and details of the request in writing. Where possible, a SAR is made in writing on the Crosscare Subject Access Request Form (see Appendix 1 here) or by email or by handwritten hard copy. The ID of the person making the SAR needs to be verified – unless there is no doubt about the person's identity. While an individual is entitled to access any or all of their personal data, where Crosscare has a large quantity of information concerning the individual, Crosscare will request that the person making the SAR clarifies what information they want. If the person refuses to clarify this, Crosscare will comply with the original request. Crosscare will respond to a SAR within 30 days / one calendar month. As appropriate, documents being given

as part of a SAR will be appropriately redacted – see here for guidance on redaction for SAR - https://www.dataprotection.ie/sites/default/files/uploads/2021-08/Redacting%20Documents%20and%20Records.pdf. Documentation will be sent to the person who requested them by registered post. If handed over in person, a person will sign to verify they received the documents. If documents are being emailed the person will be asked to confirm receipt by email. The RoPA will indicate data types held on the data subject. Unstructured data , e.g. emails mentioning the data subject, need to be included in the SAR also.

- Right to Complain, Right to Judicial Remedy: where a Data Subject is not satisfied that Crosscare adhered to its obligations under the GDPR, he or she can consider bringing a complaint to the Data Protection Commissioner or seek a judicial remedy in the Irish courts.

Data Protection by Design and Default:

The GDPR contains the new concepts of privacy by design and by default, intended to strengthen the protection of privacy by requiring organisations to build consideration of privacy into their product and service design processes in certain cases. Privacy by Design requires organisations to consider privacy measures during product design processes, while Privacy by Default requires controllers to ensure that, by default, only necessary data is processed. **Data Protection Impact Assessments (DPIAs)** must be carried out prior to any new development, system change or operational change to ensure these developments are in line with the 'by design and default' requirement. The Data Protection Commission provides clear guidance on DPIA implementation.

Data Breach:

Crosscare holds, processes and shares a large amount of personal and sensitive data which needs to be suitably protected. Every care is taken to protect this personal and sensitive data from incidents, either deliberate or accidental, to avoid a data protection breach.

Art. 33 of GDPR states that *'in the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.'*

It is assumed all breaches are reported to the DPC *'unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.'*

Any individual who accesses, uses or manages Crosscare's information is responsible for reporting a data breach and information security incidents immediately to their line manager, senior manager and the senior manager responsible for data protection, Yvonne Fleming (contact yvonnefleming@crosscare.ie) using the Crosscare Data Breach Incident Notification Form (see Appendix 2).

Appropriate steps will be taken immediately to minimise the effect of the breach, assess how/why it happened, take steps to mitigate such a breach being repeated and notify all relevant parties of the breach. **The relevant manager, senior manager and the senior manager responsible for data protection, Yvonne Fleming, will assess if a report to the Data Protection Commissioner is required.**

Crosscare is obliged under the GDPR to have in place procedures to ensure the security of all personal data during its lifecycle. See Section 3, part 6 of this document and the bespoke GDPR procedures for each part of Crosscare.

A data breach includes but is not restricted to:

- Loss or theft of personal data or equipment on which such data is stored (e.g. loss of laptop, USB stick, iPad/tablet device or paper record)
- Equipment theft or failure
- Unauthorised use of, access to or modification of data or information systems
- Attempts (failed or successful) to gain unauthorised access to information or IT systems
- Unauthorised disclosure of personal data
- Website defacement
- Hacking attack
- Unforeseen circumstance such as a fire or flood
- Human error
- 'Blagging' offences where information is obtained by deceiving the organisation that holds it

Data exchange relationships:
There are different data exchange relationships e.g.:Crosscare (as Data Controller) exchanges data with another company which processes personal data on Crosscare's behalf or Crosscare collaborates on a peer-to-peer basis with another organization to achieve a particular objective (both parties retain their Data Controller status).
All data exchange relationships need to be documented covering:

- roles and responsibilities of each party to the agreement
- how data subject rights will be managed between the two parties
- point of contact for data subjects to reach out to in the event they wish to exercise any of their data protection rights
- signature of all parties.

A memorandum of understanding or service level agreement (which covers matters other than GDPR) can include the GDPR requirements also – a separate document may not be needed. NOTE: if Crosscare is exchanging data with another org. in a case relating to an individual, that individual's consent covers GDPR requirements and a data exchange agreement is not needed.

Records of Processing Activities Log (RoPA):

All data processing activities need to be logged in a transparent and auditable manner in a spreadsheet. The Crosscare Records of Processing Activities Log (RoPA) is collated by the Crosscare overall Data Protection lead and offers a consolidated view of the various

processing activities around the organisation. Crosscare Senior managers, managers and Crosscare project/support area data protection reps. will be periodically requested to update the Crosscare Records of Processing Activities Log (RoPA). The RoPA can assist in Subject Access Requests where it summarises all data categories held.

Communications:

In promoting our work online and in print, we regularly use videos, photos and testimonies from staff and service users. Consent must always be sought before taking and publishing images and other personal information.

- The most efficient approach to obtaining consent is to record permission through general application forms when a young person or service user first connects with Crosscare and update on an annual basis.
- Where a person's image and/or personal data is required for a large-scale project (e.g. website, posters, reports, media packs), they must be informed and understand how and where their image may be used. Written consent must be obtained in advance using the Media Consent Form (Appendix 3) This form must be stored for at least one year.
- If someone wishes to withdraw their consent for the use of their image/personal data this should be obtained in writing or e-mail and communicated promptly via e-mail to the relevant manager and Senior Manager for Communications. In so far as possible, images and data should then be deleted.
- For once-off/short-term work (current social media postings) those taking part must be clearly informed where their image and data will be used. Verbal consent must be obtained from adults in these cases.
- Images used online for an extended period (over one year) should be regularly reviewed to determine if they should be updated or removed if the subject is deceased.
- For staff members, it is understood that as part of your work with Crosscare, you participate and consent to have your data used to promote the work of the wider organisation. If a staff member requests <u>not</u> to have their image used, this should be noted by the relevant manager and communicated to the Senior Manager for Communications.
- Gardai and CCTV – where Gardai seek to view Crosscare CCTV this is to be allowed. Where Gardai seek a copy of Crosscare CCTV footage this is to be requested in writing.
- GDPR introduces a number of specific requirements relating to the processing of children's data:
    - 16 years is the digital age of consent in Ireland
    - Where the child is below the age of 16, such processing shall be lawful only if the holder of parental responsibility over the child gives consent. Preventive or counselling services offered directly to children are exempted from the requirement for parental consent as they seek to protect a child's best interests.
    - Crosscare will ensure that the provision of information to data subjects is provided in a concise, transparent, intelligible and easily accessible form,

using clear and plain language – this is especially important in respect of information addressed specifically to a child.

Section 5 - Roles and Responsibilities

Crosscare Senior Managers (SMs):

Crosscare's management structure comprises a CEO to whom four senior service managers and directors of finance and HR answer. The CEO answers to the Crosscare Board.

Crosscare overall data protection lead:

Crosscare's overall data protection lead is a member of the Senior Management Team and, as such, answers directly to the CEO.

Crosscare project/support area data protection reps.:

For each project and support area of Crosscare (page 2 above) there is a data protection rep.

Staff Members:

Crosscare staff members are responsible for ensuring that all data that they access, manage and control as part of their daily duties is done in accordance with this policy and the relevant set of procedures. Crosscare staff members must also ensure their personal information provided to Crosscare is accurate and up-to-date (e.g. informing Crosscare of change of address or other circumstances). Failure to comply with this policy may result in a breach of GDPR exposing Crosscare to litigation from an injured party. All current and former staff members of Crosscare will be held accountable, from a disciplinary perspective, in relation to all data processed, managed and controlled by them during the performance of their duties in Crosscare. Failure to follow these guidelines may be regarded as a breach of this policy and may be subject to disciplinary action up to and including dismissal.

Data Protection Commissioner:

The Commissioner is appointed by Government and is independent in the exercise of his or her functions. Individuals who feel their rights are being infringed can complain to the Data Protection Commission (DPC), who will investigate the matter, and take whatever steps may be necessary to resolve it. The DPC is a good source of guidance on all data protection matters. See www.dataprotection.ie

Section 6 - Advice/Assistance

For in-house advice or assistance please contact:

- your Crosscare project/support area data protection rep.
- your line manager
- Yvonne Fleming, Senior manager (Crosscare overall data protection lead), yvonnefleming@crosscare.ie

Externally, the Data Protection Commissions office is contactable at info@dataprotection.ie / Lo Call no.1890 252 231 / www.dataprotection.ie / www.GDPRandYOU.ie

Appendix 1 – Crosscare Subject Access Request Form

1. Name, Address, Phone no., Email address (so we can get in touch with you in relation to your request)

2. What is your link to Crosscare – staff, volunteer, service user? Please give details

3. Is the information about you? If yes, you will need to provide a copy of photographic ID, bearing your signature, for example, a passport or driving licence. We will retain this until we have completed your Subject Access Request.

4. Please describe what information you require with any additional facts that may help us with the search.

5. **Declaration to be completed by all applicants.**

   I, _____ (name), certify that the information given on this application to Crosscare is correct. I understand that it is necessary for Crosscare to confirm my identity and it may be necessary to obtain more detailed information in order to locate the correct personal data.

Signed _____ Date _____

Note: Crosscare must respond to your request within one calendar month/30 days. This time frame will not begin until your identity has been established and any relevant details obtained.

Please return the completed form and any necessary documentation to **the relevant project manager, senior manager OR Crosscare overall data protection leader, yvonnefleming@crosscare.ie**

Crosscare will process the personal information included on this form in accordance with GDPR.

Appendix 2 –Crosscare Data Breach Incident Notification Form

Data Breach Incident Notification Form

The purpose of this document is to report a Breach Incident involving Personal Data, as required under General Data Protection Regulation from 25 May 2018. Crosscare is committed to protecting the confidentiality and integrity of the personal information under its control and will ensure that such incidents are appropriately investigated and reported, and that the risk of a recurrence is minimised.

****PLEASE FILL IN ALL PARTS OF THIS FORM****

Contact Information

Data Controller/Organisation:	Crosscare
Crosscare overall data protection lead:	Yvonne Fleming
Contact details:	yvonnefleming@crosscare.ie 087 7696502

High Level Description of Incident

Brief Description of Incident:		
Date of Incident:		
Location of Incident (if known):		
Date and time when Controller was made aware (if different):	**Date:**	**Time:**

Personal Data Impacted by Incident

Description of Personal Data / Sensitive Personal Data impacted:	
Categories of Data Subjects	

impacted:	
Volume of records involved:	
Number of Data Subjects impacted:	

Detailed Description of the Incident

(Description of the sequence of events leading up to the breach incident - please include associated e-mail correspondence)

Actions taken (to date) to address the Incident

(Description of the measures which have been taken since becoming aware of the Incident)

Current Status (At time of reporting)

(What is the current status of the Personal Data impacted by the breach incident?)

Actions being taken to minimise impact on Data Subjects

Action	Description	Owner	Status (planned, under way, complete)

Actions being taken to prevent a recurrence of the incident

Action	Description	Owner	Status (planned, under way, complete)

Reporting to External Agencies or Individuals

(Where information on the incident has been communicated to an external party, either corporate or individual, please attach a copy of the communication)

External agency 1	
Details of Reporting Obligation (Regulatory, Legal, Data Subject, Insurance)	
Date of Incident Notification	
External agency 2	
Details of Reporting Obligation (Regulatory, Legal, Civil, Insurance)	
Date of Incident Notification	
External agency 3	
Details of Reporting Obligation (Regulatory, Legal, Civil, Insurance)	

Date of Incident Notification	

Appendix 3 – Crosscare Media Consent Form

Consent Form for photography/audio/video

I agree for my name, photograph, video footage, or audio to be taken by Crosscare for use in online and print publications to promote their work in the community.

- Event: _____
- Location: _____
- Date: _____

Here are some places Crosscare might use your image and information:

Social and Digital: Website, Twitter, Facebook, YouTube, Instagram, Tik Tok and any other Crosscare social media accounts.
Media: National, regional and local media (broadcast, online and print).
Publications: Annual reports, newsletters or policy documents.

To do this, we must process and store your information in line with our Data Protection Policy on www.crosscare.ie. You can change your mind and withdraw consent for us to process your photograph, audio or video at any time by contacting info@crosscare.ie / 01-8360011. Your participation is entirely voluntary, and you are not obliged to consent to have your voice or image captured. No fees will be paid to people taking part. Please indicate your consent (or your consent on behalf of your child if applicable) for this photography/audio/video footage and that you fully understand the proposed use of the photography, audio or video by signing below.

Signature:

_____

Contact Number: _____

Email address: _____