Data Protection Handbook

GDPR

"It's everyone's responsibility"

A practical guide for Brothers of Charity Services staff to the Data Protection Act 2018 & The General Data Protection Regulations (GDPR)

V2 June 2020

Table of Contents

'Staff must only access the files and information of any person supported or employed by BOCSI on a "need to know" basis and should only view data that is relevant or necessary for them to carry out their duties.'

1. Introduction

Data Protection – A Commonsense Practical Approach

1.1 In the course of their work, staff and sometimes volunteers are required to collect and use certain types of information about people, including 'personal and sensitive data' as defined by the Data Protection Act and the European Union, General Data Protection Regulations (GDPR). Collecting, organising, using, and filing this data is called 'data processing'. This information can relate to the people we support and their family members; current, past and prospective employees; suppliers; other service providers; external contractors; volunteers; students; interns; and others with whom the Brothers of Charity Services Ireland (BOCSI) communicate. In addition, staff may occasionally be required to collect and use certain types of personal information to comply with the requirements of legislation. The BOCSI creates, collects and processes a vast amount of personal data in multiple formats every day and has a responsibility to comply with Irish Data Protection Law and GDPR.

1.2 The people we collect data from are called 'data subjects' and they have rights under GDPR and the Data Protection Act (2018). BOCSI as an organisation that processes personal and sensitive data in order to carry out their work is called the 'Data Controller'. As the Data Controller we are obliged to ensure that every Data Subject is informed of their rights set out in the GDPR and the Data Protection Act (2018). In order to comply with this obligation the BOCSI have produced a leaflet which must issue to all new Data Subjects or their parents or guardians at point of entry to the Service. (See Appendix 1 for leaflet).

2. Transparent, Fair, and Lawful

Transparent: *Tell the person whose data it is (the data subject) that BOCSI are collecting the data/information, why it is necessary to keep this information, how long we will keep it, who we will share it with, and how it will be safely stored.*

Fair: *What we do with the data must match up with how we have described it to the data subject.*

Lawful: *Processing must meet the correct lawful purpose.*

2.1 Lawful Basis

2.1.1 The GDPR require a lawful basis for the processing of data to be legitimate. There are six separate considerations, and the BOCSI would normally use Vital Interests, Legitimate Interests and even a Public Task for those we support (See Appendix 2 for further details).

2.2 Purpose Limitations

2.2.1 Personal data can only be used for the purpose for which it was originally obtained and must be for "specified, explicit and legitimate purposes". For the BOCSI that is the provision of services, to comply with contracts, and to comply with employment and other legislation.

2.3 Data Minimisation

2.3.1 Data collected on a person should be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed i.e. no more than the minimum amount of data should be kept for specific processing.

2.4 Accuracy

2.4.1 It is incumbent on BOCSI staff to ensure the collection of accurate data for efficient and effective decision making especially in cases of emergency. Data must be "accurate and kept up to date". All BOCSI staff must:

- *Take reasonable steps to ensure the accuracy of the personal data they have obtained.*
- *Consider whether it is necessary to update the information, especially if the data is time-sensitive (i.e. likely to become inaccurate over time unless it is updated).*
- *Verify that manual and computer procedures ensure high levels of data accuracy. Be aware of different software versions e.g., Excel 2007, 2010, 2013. If you are unsure, please ask your line manager or your local ICT personnel.*
- *Think about how you keep the personal data you hold up-to-date. Is this done on a set time frame? (e.g. once a month, year or on renewal of a contract for example).*

2.4.2 To comply with the accuracy requirements of GDPR, the BOCSI must ensure the following.

- *Clerical and computer procedures are adequate, with appropriate cross-checking to ensure high levels of data accuracy.*
- *The general requirement to keep personal data up-to-date has been fully communicated to all staff through the regional Data Protection Representative and the Data Protection Officer.*
- *Appropriate procedures are built in to records management, including periodic reviews and audits.*

2.5 Storage Limitations

2.5.1 The Data Protection Commissioner expects personal data to be "kept in a format which permits identification of the individual person only for as long as is necessary" based on the legal requirement to hold the information. Data no longer required should be removed in accordance with the BOCSI Records Management and Retention Policy. All staff must have read and understood the BOCSI Records Management & Retention Policy.

2.6 Integrity and Confidentiality

2.6.1 This requires processors (staff members) to handle data "in a manner ensuring appropriate security of the personal data including protection against unlawful processing or accidental loss, destruction or damage".

2.6.2 All staff working in the BOCSI are legally required under the General Data Protection Regulations 2018 (GDPR) to ensure the security and confidentiality of all personal and sensitive data they collect and process on behalf of the people we support. This also applies to current, past and prospective employees, suppliers, service providers, external contractors and others with whom the BOCSI communicate. Data protection rights apply whether the personal data is held in electronic format (on a pc/laptop/recorder) OR in a manual format (paper file/post it note/note book/diary).

2.6.3 National ICT provides support for all data bases and IT systems within the BOCSI. Do not use any IT packages or IT systems not supported by National ICT. If you are using any package which is not currently supported by National ICT please inform your local IT staff member immediately.

2.6.4 Do not use personal email or personal phones to exchange BOCSI work data.

2.6.5 Mobile phones, i-pads, tablets, USB keys, recorders, lap tops, hard drives (PCs), SD cards, e-mails, cameras, and any other form of assisted technology including, door alarms, epi watches, video call bells, and personal activity trackers all hold data. Electronic devices should be stored in a secure way and must be password protected or encrypted as appropriate. If an electronic device is lost or stolen, please contact ICT immediately as they can remotely shut down some of these devices to prevent a data breach.

3. Data Breach

3.1 What is a Data Breach?

1. Accidental destruction of data.
2. Deliberate destruction of data.
3. Loss of data.
4. Unauthorised alteration of data.
5. Unauthorised processing of data.
6. Unauthorised disclosure of data.
7. Unauthorised removal of data.

3.2 What is Personal Data?

3.2.1 Under GDPR, "'Personal data' refers to any data which concerns a living person who is or can be identified either from the data itself or from the data combined with any other information that is or could come into the possession of the data controller". In other words, any information that is clearly about a particular person. In certain circumstances, this could include anything from someone's name to their physical appearance. This information should be protected and only shared with colleagues in a secure way and only as required by your work.

3.2.2 Data that is considered personal data including sensitive data, either on its own, or in combination with other data:

- *Biographical information or current living situation, including dates of birth, Social Security numbers, phone numbers and email addresses.*
- *Looks, appearance and behaviour, including eye colour, weight and character traits.*
- *Workplace data and information about education, including salary, tax information and student numbers.*
- *Religion, political opinions or affiliations and geo-tracking data.*
- *Health, sickness and genetics, including medical history, genetic data and information about sick leave.*

3.2.3 All of the following are considered personal data:

- *John Murphy*
- *John.murphy@BOCSI.ie*
- *PPS Number 1234567a*
- *@johnmurphy10*
- *John Murphy, No. 1 Cork Rd, Dublin*
- *087 5552222/01 5552222*

3.3 What is Sensitive Data?

3.3.1 Sensitive data refers to data that must be treated with extra security includes,

- *Racial or ethnic origin;*
- *Political opinions;*
- *Religious or philosophical beliefs;*
- *Trade union membership;*
- *Sexuality;*
- *Genetic[*] data; and*
- *Biometric[**] data.*

[*]*Genetic data - means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question such as DNA.*

[**]*Biometric data - means personal data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as fingerprints and facial images.*

3.4 Securing Sensitive Data

3.4.1 This data should be held in a secured/locked drawer or filing cabinet, separately from other personal data, with restricted access. As with personal data generally, it should only be kept on electronic devices if the device is secure and password protected. It is good practice to pseudonymise[*] files which contain sensitive data.

[*]*"Pseudonymisation" of data means replacing any identifying characteristics of data with a value which does not allow the Person(s) to be directly identified. But whereas pseudonymisation allows anyone with access to the data to view part of the data set.*

3.5 Breach Incident Procedures - Identification of an Incident

3.5.1 Follow the Data Breach Procedures. As soon as a data breach has been identified, if you can contain the breach do it immediately for example, recall the email, contact IT to recall the email or to shut down a phone. Contact the person to whom you sent the email and request that they delete it off their system including their wastepaper basket/deleted items folder. If you receive notification from a person that they received a hard copy letter/report in error please organise to collect the data from them as soon as possible or request that they return the letter/report to you and confirm that no other copies have been made or shared.

Report the breach to your direct line manager and the Regional Data Protection Representative immediately so that breach procedures can be initiated and followed without delay. Remember that once the breach is identified the clock starts to tick on our responsibility to report to the Data Commissioner's Office within 72 hours of the breach being discovered.

If your line manager is not available go straight to the Data Protection Representative in your Region. If they are not available report the breach to the BOCSI Data Protection Officer on 076 1064323 or 087 915 7560. Repeated breaches by the same staff member may result in disciplinary procedures following a review of each incident/breach.

3.5.2 Once the Data Protection Representative is satisfied that a breach has occurred, they then report that breach to the Data Protection Officer. The DPO will establish if the breach is reportable to the Data Protection Commissioner, and if so will report to the Data Protection Commissioner within 72 hours of the breach being identified.

3.5.3 Reporting incidents in full and with immediate effect is essential to the compliant functioning of BOCSI and is not about apportioning blame. Please use the Data Breach Procedure Form (See Appendix 3). You can get a copy of this form by email from your DPR or the DPO.

4. Protection of Data

4.1

Personal or sensitive information MUST not be deliberately or inadvertently viewed by those who do not require access to it to do their job.

- *Staff must only access files and data relating to the people we support on a "need to know" basis and should only view data that is relevant or necessary for them to carry out their duties.*
- *It is not acceptable for any sensitive or personal data to be left unattended, in or around a printer/photocopier. Staff who send sensitive personal data to a printer MUST attend to/pick up the data immediately.*
- *If you find personal or sensitive data on a printer/photocopier please remove it immediately and bring it to the attention of your line manager as this constitutes a data breach.*

- *Staff should operate a 'Clear Desk policy'. This means that at the end of each working day and when away from their desk / area of work for any period of time your desk is clear of paper and your electronic devise is password protected (locked or switched off).*
- *Personal and sensitive records held on paper and/or screens in your office / work area must be kept concealed from callers to your office / work area (e.g. unexpected caller – turn applicable paper over to obstruct view and switch off the screen.)*
- *Any files containing personal / sensitive information must NEVER be left unattended, where they are visible or may be accessed by unauthorised staff or members of the public.*
- *If computers or VDU's are left unattended, staff must ensure that no personal information may be observed or accessed by unauthorised staff or members of the public. (e.g.: press Ctrl + Alt +Del as per 4.3.5).*
- *The use of secured screen savers is advised to reduce the chance of casual observation.*
- *Offices, rooms, filing cabinets, drawers etc. in which personal records are stored should ALWAYS be locked when unattended.*
- *A record tracing/tracking system should be maintained to identify files removed, by whom, and when they are returned.*
- *Discussions in relation to persons supported and/or staff should not be held in open areas, where it is possible to be over-heard. This includes telephone calls.*
- *If a file is being transferred to another agency, a record must be kept of the file number, unique identifier, name of individual, date of birth, name of person and contact details of agency the file is being transferred to, and the date on which it was transferred and by whom within BOCSI.*
- *If a file is being destroyed, under the Records Management Policy, a record must be kept of the file number, unique identifier, name of individual, date of birth, reason for destruction, name of person within BOCSI who made the decision to destroy the file and the date of destruction.*
- *Your email is not a filing system. If electronic copies of reports and attachments or emails are required please copy these into a file on your PC and delete from your email. Email management is an essential part of good data management.*

4.1.1. Do not leave information/data unattended in cars or buses. The general rule is that staff must not take any work-related files, papers or notes from the office/place of work. In circumstances where staff are undertaking home visits, or leaving from home early the next morning to attend a meeting staff must not leave any work-related files and/or laptops, portable electronic devices containing personal information, unattended in cars and BOCSI vehicles. In cases where staff remove an individual's files/records/charts from their office/place of work to attend meetings, clinics, home visits, etc. these documents MUST always be carried in a suitable case/bag to avoid any unintended viewing and also to secure the documents. A note should be left on the file in the office/place of work to identify what files have been removed and by whom.

4.1.2 All documents, including any portable equipment MUST be stored securely. If files containing personal/sensitive information MUST be transported in a vehicle, they must be locked securely in the boot for the minimum period necessary. Staff should not take health care records home however in exceptional cases, where this cannot be avoided, these records MUST be stored securely indoors and never left in cars overnight.

4.1.3 It is essential when remote working or working from home during a crisis (e.g. covid-19) that you comply with all data protection policies including the BOCSI Remote Working Policy & Procedure (2020).

4.2 Information Sharing/Messaging Platforms

4.2.1 The use of WhatsApp for any BOCSI business is prohibited, (this includes sharing staff rosters, individual's appointments, photos, or details of an individual's day). The transfer of personal or sensitive information via WhatsApp is a breach of GDPR and must be reported to the Data Protection Representative in your Region or the Data Protection Officer.

4.2.2 ICT has suggested alternative systems which are GDPR compliant.

- Microsoft Teams which is installed on your PC or Laptop you can request ICT to support you to add a particular Team or you can create your own team on the system.

- 'Microsoft Kaizala for Business' which operates similarly to WhatsApp (You can download this from the App Store for free for your mobile phone). Each Group requires at least one administrator, please identify your Region/Area to avoid any national overlaps in the Group name. The Administrator (person who sets up the Group) should keep a list on an excel spread sheet of the name of the group, date the group was set up, names of people in the group, the purpose of the group, and the name and date that any person has been removed from the group.

4.2.3 The information on these systems is stored in Ireland or another country in the EU making them compliant with GDPR. It is essential that when a staff member moves area/leaves/retires that they are removed from any Groups/Teams by the Administrator. (see BOCSI National Exit Protocol 2020).

4.3 Clear Desk Guidance

4.3.1 Under Data Protection Regulations as of May 25th 2018, sensitive information MUST be protected at all times from anyone who may walk by, such as other employees, office visitors, and cleaners.

4.3.2 At the end of the work day, all confidential data should be returned to a locked drawer or filing cabinet. When a workspace is left even for a quick break, precautions like locking the pc, locking the office door, and putting away any sensitive data must be taken. The best practice is to file away or lock up sensitive information and switch on the computer's password-protected screen saver.

4.3.3 Benefits of a Clean Desk set up

- ***Information security:*** *At the top of the list, a Clean Desk helps protect sensitive information and reduces the risk of a data breach and identity theft.*
- ***Compliance:*** *A Clean Desk supports an organisation's compliance with GDPR.*

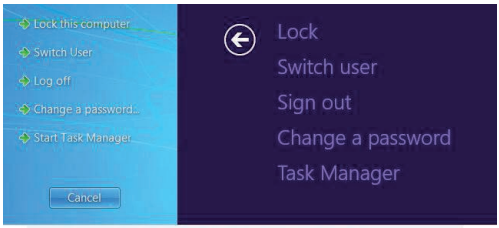
- ***Flexible working:*** *The policy supports 'hot desking', which is an office design system where employees do not have assigned desks, aiding flexibility in the workplace. All desks are left empty every evening and employees can sit where they want as they arrive in the morning. A Clean Desk policy is particularly important when 'hot-desking' is in use.*
- ***Embedded security:*** *A Clean Desk helps create security-driven work habits. The goal is for employees to start their day by planning and organising documents needed for their immediate work. If an employee has to attend a meeting or take a break, it should be HABIT to do a quick check first to see if there is sensitive information on the desk – and secure it.*

4.3.4 Whether you have an allocated desk, an office or work in a hot desk area, maintaining a clear desk supports security, cleanliness, and allows others to use the available space. Adopting a clean desk approach will help reduce the risk of unauthorised access to sensitive and confidential documents and data.

4.3.5 Follow the 3Ps - PLAN, PROTECT and PICK UP

Step 1. **PLAN** first thing in the morning. Keep the things you need for your workday on your desk. File all other folders and documents in locked storage, but don't leave the key in!

Step 2.



PROTECT information whenever you leave your desk. Do not leave confidential or sensitive information unattended on your desk, lock it away, or lock your office door. In addition, if you are not taking your device with you, lock it using one of the following:

For Windows Users - pressing the Window and L keys at the same time

Pressing Ctrl + Alt + Delete keys at the same time and choosing the "Lock this Computer" or "Lock" option

Step 3. **PICK UP** at the end of the day. When you leave in the evening, do not leave documents out or whiteboards with information or data on them. It is essential to file away your documents in locked storage or if no longer required - shred them. If you get into the habit of cleaning off your desk every day before you leave, you'll enjoy the added productivity benefits that come with a clean desk or office first thing in the morning!

4.4 Social Media

4.4.1 It is not permitted to use social media platforms to share information regarding your work or the people you work with; this includes photos of your colleagues, or the people you work with, or your place of work.

4.5 Frequently Asked Questions

Q. ***How do I lock my screen before I move away from my device?***

A. Pressing the Window-L keys together, the Ctrl-Alt-Delete keys at the same time and choosing the "Lock this Computer" or "Lock" option or by using the function from the start menu.

Q. I don't have any personal filing space, what should I do?

A. All personal filing and items should be locked away each night into your allocated storage. If you do not have personal or team filing space please bring it to the attention of your line manager.

Q. May I set up a Facebook Page, Twitter or YouTube account for a project?

A. Yes you may, but you must have written permission from your Director of Service and you must ensure that no personal or sensitive data is placed on the site without the express consent of the data subjects.

5. Sharing Personal and/or Sensitive Information

5.1 Email Data - Password Protection

5.1.1 Personal or sensitive information should at all times be sent in a password protected document. Please do not send a second email with the password. Please text or make a telephone call to the receiver informing them of the password. The sender of the information is responsible for password protecting documents. This prevents a data breach, in the case of one using an incorrect email address or sending the e-mail to the wrong person.

Steps to Password Protect your document

- *Open your Microsoft Word document. Double-click the Word document that you want to protect with a password...*
- *Click File. It's a tab in the upper-left corner of the Word window...*
- *Click the Info tab...*
- *Click Protect Document...*
- *Click Encrypt with Password...*
- *Enter a password...*
- *Click OK...*
- *Re-enter the password, then click OK.*

Please ensure that if you are forwarding an email or responding to an email that only the information required to issue to the receiver is contained in the email; avoid issuing 'chain emails' unless the previous emails are necessary for the understanding of the receiver.

5.1.2 GDPR define sensitive data as,

(a) Persons racial or ethnic origin, their political opinions, or their religious or their philosophical beliefs;

(b) Whether the data subject is a member of a trade union;

(c) The physical or mental health or condition or sexual life of the data subject;

(d) The commission or alleged commission of any offence by the data subject; and

(e) Any proceedings for an offence committed or alleged to have been committed by the data subject, the disposal of such proceedings, or the sentence of any Court in such proceedings.

5.1.3 Please double check that you have the correct email addresses before you press the send button. If you are unsure of the email address please send an email to the address requesting a return email confirming the address.

5.1.4 Staff must respect the Privacy of others at all times, and access email messages only where they are the intended recipient or have a valid work-related reason. If a Staff member(s) receives an email message and they are not the intended recipient they must immediately make contact with the sender and notify them of the error.

5.1.5 It is ONLY acceptable to send confidential and personal information by Fax in a Medical Emergency, where a delay could cause harm to the Person(s) supported or in Exceptional Cases – Note: The fax machine is often used for communication of prescriptions.

5.1.6 The following steps are to be taken to maintain security and confidentiality when sending personal information by Fax in Emergencies or Exceptional Cases.

- *The fax message must include a The BOCSI fax cover sheet.*
- *Only the minimum amount of information necessary should be included in the fax message. Before sending the fax message, ensure to contact the intended recipient to confirm they are available to receive the Fax at the agreed time.*
- *Ensure that the correct number is dialed by sending a test sheet.*
- *Keep a copy of the transmission slip and confirm receipt of the fax message.*
- *Ensure that no copies of the fax message are left on the fax machine.*

5.1.6 When using An Post / Courier, mail containing sensitive personal information MUST be stamped "Strictly Private & Confidential". If proof of delivery is necessary, information of this nature MUST be sent by registered post.

5.1.7 Ensure "return to sender" information in the event that the mail is undeliverable. Please check the individual's unique identification number and that the name on the letter/report corresponds with the name on the envelope. The use of envelopes with windows can reduce the possibility of letters being misdirected.

5.1.8 Please remember that you are responsible for the confidentiality of any data you hold on electronic devises (i.e. mobile phones, i-pads, tablets, USB keys, recorders, lap tops, hard drives (PCs), SD cards, e-mails, cameras, and any other form of assisted technology including, door alarms, epi watches, video call bells, and personal activity trackers).

5.1.9 Please return all devices to your line manager or ICT when either leaving or changing your job or obtaining an up-grade. This is to ensure that any data remaining on the device is wiped clean under confidential conditions.

5.2 Organisations providing services on behalf of BOCSI – Joint Processor

5.2.1 Where the BOCSI engages a third party to provide services on its behalf, and where the services require the third party to process any personal or sensitive data , the BOCSI is required by the GDPR to have a written contract in place, called a 'Joint Data Processor Agreement' which provides written guarantees with regards to GDPR. A standard joint data processor agreement is available from your DPR or the DPO. Relevant Data Protection documents are also available to download from Privacy Engine which is the IT tool the BOCSI use to record all data protection related information.

5.3 Policies

5.3.1 The Brothers of Charity Services Ireland has the following related policies & procedures:

- *Data Breach Notification Procedure;*
- *Subject Access Request Procedure;*
- *National Records Management & Retention Schedule Policy;*
- *National Exit Protocol 2020;*
- *Confidentiality Policy; and*
- *BOCSI Remote Working Policy (2020).*

5.3.2 All records generated by staff when carrying out their work for BOCSI are the property of the BOCSI.

5.4 Data Retention & Disposal

5.4.1 BOCSI have defined procedures for adhering to the retention periods as set out by the relevant laws, contracts, and our service requirements, as well as adhering to the GDPR requirement to only hold and process personal information for as long as is necessary. All personal data is disposed of in a way that protects the rights and privacy of persons/data subjects (e.g. shredding, disposal as confidential waste, secure electronic deletion, archiving etc.) and prioritises the protection of the personal data in all instances.

6. Data Protection Impact Assessment

6.1

BOCSI as a Data Controller is required under GDPR to carry out Data Protection Impact Assessments (DPIM) where processing is likely to result in "high risk". The Term 'Privacy Impact Assessment' is interchangeable with DPIA. DPIAs are undertaken by the project lead in consultation with the Regional DPR.

6.2 Undertaking a DPIA

6.2.1 This assessment is required at the beginning of any proposed major project/system, or a change to an existing project/system, which involves processing of personal information. BOCSI ICT require that a signed off DPIA is submitted along with a change or development order before they will make changes to any system involved in the processing of sensitive data.

- The DPIA should ensure that any identified risks to the personal information will be considered, evaluated and appropriately managed in this project/system.
- It must be undertaken by the individual/project team proposing the project/system/change.
- The Data Protection Representative (DPR) in your Region must be consulted in the completion of this form and is happy to assist you as required.
- It can be submitted and subsequently re-assessed in light of changing information.

6.2.2 The BOCSI have a standard form to aid the project lead to undertake a DPIA, (See Appendix 4(a)). For an amendment to any ITC Systems or a new ITC system use the ITC 'Change Request Form', Section 3 of this form covers the requirement for a DPIA (See Appendix 4(b)). This form will not be published but will be maintained on a file in Privacy Engine for the purposes of GDPR compliance. The Regional DPR will support you in undertaking DPIAs and will upload a copy of the form to Privacy Engine once it is signed off.

6.2.3 It is important to note where safeguards to mitigate risks cannot be determined, or risks remain high, the Data Protection Officer must be notified by the DPR who in turn must notify the Data Protection Commissioner in advance of undertaking the processing. The Data Protection Commissioner may direct that we do not carry out the proposed project/process in full or in part.

7. Review

7.1

This handbook will be reviewed in 3 years unless an audit, serious incident, organisational structural change, scope of practice change, advances in technology, significant changes in international best practice, or legislation, identifies the need to update the handbook sooner.

The original Handbook was researched, drafted, and produced, by the BOCSI DPO and the National Data Protection Team (May 2018). This is version 2 - reprinted with additions in June 2020.

Appendix 1

To: Individuals who are supported by the Services of the Brothers of Charity Services Ireland

How does change in Data Protection affect you?

Data Protection means that your personal information is stored properly

On 25th May 2018 a new EU rule came in to effect called the General Data Protection Regulation or GDPR

This is an update to the existing data protection law
It makes all Organisations including the BOCSI more accountable for what they do with your information.
It gives you more control over what we do with your information.

The Brothers of Charity Services Ireland must collect and keep personal information about you to help us provide you with a good service. To know who to contact in an emergency.

This information includes:

· Name
· Gender
· Date of birth

· Religion
· Address
· Phone numbers

· Next of Kin
· Medical history
· Behaviour Support Plans

· Financial details
· Multi-disciplinary Reports
· Dental and GP appointments

We must keep your information safe

Sometimes we may share your information with people. This is to make sure that we can give you the best service. People we may share information with include

· Staff who work with you

· State Bodies who may need information

· Family members who you have said we can.

· Healthcare professionals

· The Hospital

We have your information because we want to give you services and supports.

The Data Protection law says the information must be up to date.

You can see the information about you if you want to. This is your right.

We must get back to you within 30 days of you asking

If we say no to giving you the information we must tell you why

If we say no and you are not happy with this you can contact the Data Protection Commissioner.

They will check what information we have

They will ask us why we said no.

If they don't agree they will tell us to give you your information and we must do so.

You should know:

That we have personal information about you

Why we have it and What we do with it.

You have the right to ask questions about this.

If the Brothers of Charity Services Ireland want to use your information for another reason, not in connection with the supports we provide to you, we must ask you first

You can contact the Regional Data Protection Representative: (insert regional details)

Or the Brothers of Charity Services Ireland Data Protection Officer by email at DPO@bocsi.ie or post at Kilcornan House, Clarinbridge, Co Galway H91 K2E9

What are the lawful bases for processing?

The 'legal basis' also referred to as a 'lawful bases or reason' means the legal justification for the processing of personal and sensitive data. A valid legal basis is required in all cases if a data subject's personal data is to be lawfully processed in line with Article 6 of the GDPR. There are six possible legal basis and at least one of these must apply when you process personal data. There is no hierarchy or preferred option within the legal basis. The processing of personal data should be based on the legal basis which is most appropriate in the specific circumstance of that processing. It is important to note that 'consent' whilst perhaps the most well-known, is not the only legal basis for processing personal data or even the most appropriate in many cases.

(a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose. This consent must be freely given, specific, informed and unambiguous and the data subject must indicate their consent by a statement or by a clear affirmative action.

Conditions applicable to Child's consent – Where the only lawful processing condition under Article 6 for processing a child's data is consent and the processing relates to the provision of an 'information society service' directly to the child, and the child is under 16 (Section 31 Data Protection Act 2018), consent must be sought and given by a "holder of parental responsibility over the child".

(b) Contract: the processing is necessary for a contract you have with an individual or organisation or because they have asked you to take specific steps before entering into a contract. (Under Contract is usually applied to the employee/employer relationship, or subcontractors)

(c) Legal obligation: the processing is necessary for you to comply with the law (e.g. Acts and Regulations like health, employment, and financial laws).

(d) Vital interests: the processing is necessary to protect someone's life or situations which very seriously threaten the health or fundamental rights of the individual. (e.g. Health & Social Care, including People in vulnerable mental states)

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

(f) Legitimate interests: the processing is necessary for your legitimate interests 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. (This cannot apply if you are a public authority processing data to perform your official tasks e.g. this usually applies to private businesses).

For further guidance see the Data Protection Commission Guidance Note: 'Legal Basis for Processing Personal Data (12/2019)'.

Note: *The BOCSI Records Management Policy Retention Schedule (2019) makes suggestions relating to the possible lawful basis for holding records, (needless to say these may differ depending on the specific circumstances)*

Appendix 3

Data Breach Incident Form

Data Protection Representative (DPR) Details:			
NAME:		REGION:	
DATE:		TIME:	
TEL:		EMAIL:	

Incident Information:	
DATE/TIME OR PERIOD OF BREACH:	
DESCRIPTION & NATURE OF BREACH:	
TYPE OF BREACH: (Human Error or Systems Failure)	
CATEGORIES OF DATA SUBJECTS AFFECTED:	
CATEGORIES OF PERSONAL DATA RECORDS CONCERNED:	
NO. OF DATA SUBJECTS AFFECTED:	NO. OF RECORDS INVOLVED:
IMMEDIATE ACTION TAKEN TO CONTAIN/MITIGATE BREACH:	
NAME OF STAFF INVOLVED IN BREACH:	
PROCEDURE(S) INVOLVED IN BREACH:	
THIRD PARTIES INVOLVED IN BREACH:	

Breach Notifications:	
WAS THE BOCSI DATA PROTECTION OFFICER NOTIFIED?	YES/NO
WAS THE DATA PROTECTION COMMISSIONER'S OFFICE NOTIFIED?	YES/NO
IF YES, WAS THIS WITHIN 72 HOURS?	YES/NO/NA
If no to the above, provide reason(s) for delay	

Information Provided With The Notification?	Yes	No
A description of the nature of the personal data breach		
The categories and approximate number of data subjects affected		
The categories and approximate number of personal data records concerned		
The name and contact details of the Data Protection Officer and/or any other relevant point of contact (for obtaining further information)		
A description of the likely consequences of the personal data breach		
A description of the measures taken or proposed to be taken to address the personal data breach (including measures to mitigate its possible adverse effects)		
Has the Data Subject been notified?		
Has the Data Subject been notified about their right to complain?		
Has the BOCSI Data Protection Officer been copied on this Form?		
Has the Office of the Data Protection Commissioner been notified?		

Investigation Information & Outcome Actions:
DETAILS OF INCIDENT INVESTIGATION:
PROCEDURE(S) REVISED DUE TO BREACH:

STAFF TRAINING PROVIDED: (if applicable)		
DETAILS OF ACTIONS TAKEN AND INVESTIGATION OUTCOMES:		
DID THE MITIGATING ACTIONS TAKEN PREVENT THE BREACH FROM OCCURRING AGAIN? (Describe)		
WERE APPROPRIATE TECHNICAL MEASURES IN PLACE?	YES	NO
If yes to the above, describe measures Name of Manager: _____ Signature: _____		

DPR Signature: _____ Date: _____

DPR Name: _____ Authorised by: _____(DoS)

DPO Signature _____ DPO Name _____

DPR: Data Protection Representative (Regional)

DPO: Data Protection Officer (National)

DoS: Director of Service (Regional)

Data Protection Impact Accessment

From 25th May 2018, non-compliance with this requirement is an offence under the General Data Protection Regulation (GDPR) and is subject to fines from the Office of the Data Protection Commissioner.

1. What is the project / system?

   Why do we need it and what does it aim to achieve? Is this a new system or a change to an existing system? What type of personal information is processed? Will this proposal generate new personal information?

2. What is the risk? What particular part of the project / system is giving rise to the risk? (Use the BOCSI National Risk Management Policy to record and assess any identified Risks).

   Why do you need this assessment? What risks to personal data are involved in this process? How will the project/system be carried out? Will data be shared with anyone? How will data be used, stored, protected, and deleted?

3. What Region/services will be affected by this project/ system/change?

   Will it be limited to one Region/service area?

4. Risk Mitigation

   What is the benefit of this system/procedure? Have you completed a risk/benefit analysis in terms of personal data? Rate the risk. Is there an alternative system/procedure? What is the level of risk based on the likelihood of a breach?

5. Individuals/Parties affected by or involved in the process/system

   Have all impacted parties been consulted/considered in this process? If not, why not? Is legal advice required?

Sign Off and Measures / Notes

System Proposer Signature:	Date:	Comment
Director of Services/ Head of Function Signature:	Date:	Comment
Data Protection Representative Signature:	Date:	Comment
Data Protection Officer *(in the case where mitigation of risks cannot be determined or risks remain high)* Signature:	Date:	Comment

ICT – Change Request
Section 3 – GDPR DPIA

TECHNICAL MANAGER & BUSINESS REP - DPIA

Systems Affected	*[Provide Details of systems or applications affected / new applications]*		
Personal Data	*[Provide Details of type of Personal Data processed]*		
New Data Processing	*[Provide Details of any new Personal Data being processed]*		
Risk	*[Detail risks to personal data being used, modified or shared as result of change]*		
Risk Level *(Score 1 To 5 – With 5 Highest)*	Likelihood (L)		*Score Likelihood and Impact from 1 to 5. Where 5 is the highest level. Risk is Likelihood multiplied by Impact. The lowest risk is 1 and 25 is the highest.*
	Impact (I)		
	Risk (R= L x I)		

Risk Mitigation	*[Provide Detail of mitigations or alternatives to reduce the risk]*	
Affected Parties	*[Detail all Individuals / Parties / Groups affected by the change]*	
Consultation	*[Have all affected parties been consulted on the change.]*	Yes /No
	[If Not why Not?]	

Notes

Notes

PROOF