Community Chaplaincy Association

GDPR GUIDANCE FOR COMMUNITY CHAPLAINCIES

CONTENTS

Introduction to General Data Protection Requirements (GDPR)

The data protection act will be replaced by GDPR on 25th May 2018

The Information Commissioners Office (ICO) is responsible for ensuring it is implemented and will fine for non-compliance but in proportion to the breach and the resources of the organisation.

The new law builds on current DP and is about **respecting the privacy and dignity of individuals**.

It covers how we collect, store and share **identifiable personal** data about **living** clients, volunteers, staff and donors/supporters. Not anonymised data or stats.

There are **6 principles** for Data Protection

Lawfulness, fairness and transparency. Data subjects must receive information on the identity of the organisations lead person on data and the **purposes** of processing their personal data. It must be easy to understand - plain language used.

Purpose limitation. data must only be collected for the specified, explicit and legitimate purposes and not sold on/used for some other purpose. However further processing for public interest, research or statistical purposes is allowed.

Data minimisation. data must be adequate, relevant and limited to what is necessary in relation to the purpose – no speculative fishing for extra unnecessary data

Accuracy data must be up to date and updated.

Storage limitation. data must not be kept in identifiable form for longer than is necessary

Integrity and confidentiality data must have appropriate security and protection against unauthorised or unlawful access, processing, destruction and damage. Technical and/or organisational measures are necessary to comply with this requirement

Organisations are required to comply with the above and be able to **evidence they comply**.

In addition there are **8 rights** that individuals can **request**

- To be informed about what their data is being used for lawfully- where when etc
- To have access to their data within 30 days
- To have any mistakes in their data corrected within 30 days (rectification)
- To have their data erased - to withdraw their consent
- To 'port' their data to another provider *like switching energy supplier*
- To object to how their data is processed
- To have their data suspended (out of play) whilst a dispute is being processed
- To have their data processed by a human not a computer *like a benefit decision*

There are 5 reasons for your chaplaincy processing data. All are equally legitimate.

Lawful Basis	Commentary
Informed affirmed **consent** from the subject *A child under 13 cannot normally give consent it needs to come from a parent or guardian*	Clear consent to process their data for a purpose. Consent will need to be periodically refreshed especially if circumstances change and can of course trigger a request for withdrawal etc which has a capacity cost.
Contract	Data is necessary for a contract to be delivered
Legal Obligation	You might not have the consent of a person to have or share this information but the law says you must eg employment law financial law Individual rights may not apply here
Vital Interest	This is used by Police and A&E it is literally to save a life. Consent is not necessary
Public Task	This may be a statutory agreement or contract from Government to carry out. You may have a legal duty to obtain store and share this information.
Legitimate Interest *this is the most likely use in chaplaincies*	It is in the legitimate interest of the client for us to have the data eg to risk assess them in order to match them

One of these 5 will be the Lawful Basis for your chaplaincy having the personal/sensitive data.
Once you have declared your lawful basis for the data you can't change it.

<u>Sensitive Information</u>

There are 9 special categories of sensitive information which include criminal convictions, sexuality and religion. Your policies need to be explicit that you understand this kind of personal data is *particularly sensitive.*

We hold criminal convictions information in an **official capacity** by nature of a **contract** such as a Service Level Agreement with Probation/Prison/Police etc. or **legitimate Interest** in the case of self-referral before an agreement such as a mentoring contract is signed with a client.

For benchmarking exercises you would **anonymise** the data.

<u>Emailing</u>

Emailing and texting direct marketing emails or texts cannot be sent without specific consent. We need to be explicit with donors funders and supporters and ask separately about sending them information about

- ✓ work
- ✓ fundraising
- ✓ events
- ✓ volunteering

You will need to keep a record of positive responses to evidence informed opt in.

Some examples of Lawful Basis in Community Chaplaincies

DATA SET	LAWFUL BASIS	EXAMPLES/COMMENTS
Employee personal data	Contractual Legitimate interest	Eg line in job description about keeping confidentiality and data protection in both directions Eg holding the details of their next of kin in case of emergencies is personal but necessary in the delivery of a safe working environment.
Volunteers data	Contractual Legitimate Interest	Eg Volunteer Agreement their care for the client data and your care for their data Processing information such as their answers to interview questions which help you to decide if they are a suitable volunteer mentor candidate
Clients data	Contractual Legitimate interest Consent Public task	Mentor Client Agreement which includes the Privacy Notice. Client drop in or engagement before the above agreement as having this data helps you run your service/manage your capacity. The client consents to you sharing their personal data with a volunteer mentor or with a work placement provider. The client consents to appearing in a promotional video (signed form) Commissioned service - they will tell you what it is such as CRC contract
Donors data	Consent	Regular donors will need to be sent a consent email before the law changes

Most chaplaincies will define their personal data processing through **contract, consent** or **legitimate interest**.

The advantage of consent is that it upholds the principle of transparency, however, it has a capacity and therefore cost impact in terms of revisiting and unless it is clearly explained by trained staff, it may be misleading to clients as they cannot automatically withdraw their data they can only ***request to do so***. Other priority legislation may override their request. Eg you cannot erase their information if a contract with a provider says you must keep it.

<u>Security Breaches and Complaints</u>

Preparation is key to avoiding GDPR breaches in the first place. Data needs to be held and processed securely which includes

- Locked offices, locked filing cabinets
- Not leaving information on answerphones
- Staff training on safe storage and information sharing policies and procedures.
- Limiting staff and volunteer access to sensitive data

<u>IT Security</u>

- You will need a firewall and virus checks/protective software.

- You will need to automatically update on your systems (Ask your IT)
- Make sure only the right people have access to sensitive data need to know basis
- Close down your screen if you go to the loo and train everyone else to do the same
- Address personal data you post to a named person and ensure that it is securely wrapped.
- Don't share passwords – if you need passwords held make sure they are in a locked safe.
- Encrypt personal data – such as using the right secure email
- Make sure your backups are stored securely too
- Destroy and/or wipe any old devices including mobile phones destroying the sim / hardware.

Email

- Use CJSM (Criminal Justice Secure Mail) to transfer client information with HMPPS –you can get them to set you up as they will also need to evidence their compliance with GDPR
- Use BCC for multiple addresses (not CC or To as that counts as a data breach)
- Be aware and check any auto complete functions on your computer/email etc.
- If you can't get CJSM then try to use dropbox instead …ask your IT support.

General

- Make sure you have a confidential waste disposal arrangement (local council should advise you)
- Don't use insecure sites (eg look for the green padlock on the search bar)
- Discuss with staff and volunteer users and agree how your passwords are created and stored.

How do I know it is a breach?

If something happens that you are concerned about you need to start the procedure but you might not end up reporting it externally. You may just report it to your manager or trustees. Being able to evidence ongoing records of implementing a process is valuable if at some future point a breach happens.

You will need to follow the **Data Breach Policy** and use your **Data Breach Record**

You will need to adapt your **Safeguarding Policy** and **IT Policy**

Complaints

You may receive a complaint from a client volunteer or staff member about their data

- not being upheld as per the privacy notice.
- Not secure
- Inaccurate
- Disclosed to a third party unnecessarily
- Held longer than necessary
- Information being used for another purpose not agreed with the data subject.

You will need to follow your **Complaints Policy**

Having policies in place allows you to follow a structure in the case of a complaint or breach and give a standard measured agreed response. Staff and volunteers need to know the contents of the policy documents and be aware there is a procedure to follow**.**

What Next ?

(The documents highlighted in red are available in the appendix)

- Visit the ICO website and read GDPR Guide for Charities. Record in your Trustees meeting minutes that this has happened. This is part of your compliance evidence. See also Difference between DP and GDPR below to familiarise yourself with the changes.

- Register - All community chaplaincies are data controllers and need to **register with the ICO**

- Decide who will be responsible for GDPR compliance in your organisation and how this will be publicised. A data controller is more senior to a processor but just like safeguarding, upholding the principles are everyone's responsibility. A Data Protection Officer needs to be independent of the staff structure and report directly to the Board - so for most Community Chaplaincies it will make more sense to have a DP/GDPR lead instead, which can come from the staff team.

- Deliver a training session/Briefing Document to staff/volunteers explaining about GDPR especially principles and rights, your consent agreements, SARs and data breach protocols.

- Audit the personal data you currently hold by against the 6 principles and the 8 rights. Record that this has happened using a written Data Audit Document. This is part of your compliance evidence. Remember anonymised data can be retained. This should result in you identifying unnecessary electronic and paper files that you can delete in a controlled way.

- Produce a Lawful Basis Reference Document showing under which lawful basis you are processing the personal and sensitive data you collect.

- Review your Consent Agreements for personal data from clients, volunteers, staff and donors and update them with the correct compliant text.

- Review your external contracts and service level agreements - What are they doing about GDPR?

- Update your Privacy Notices

- Update your policies and procedures to say GDPR not DP and make sure your policies have a review date on them. Pay attention to Safeguarding, IT Security including BYOD and encryption, Information Sharing and Vulnerable Adults policies.

- Be equipped to deal with SARs 'subject access requests' within 30 days

- Be equipped to detect, report and investigate Data Breaches within 72 hours

Appendices

1 The Differences Between Data Protection and GDPR (from ICO)

DATA PROTECTION ACT	GDPR
EU member states created their law around data protection	A unified approach across all member states – the UK will continue to be part of the GDPR even after departing the EU.
Covers Personal Data and Sensitive Personal Data	Covers Personal Data and Special categories of Personal Data – now includes biometric and genetic data and online identifiers.
Data Protection Officer is not required in an organisation	Data Protection Officer is required for Public Authorities (e.g. local councils, regional government) and organisations where core activities consist of processing, on a large scale, special categories of personal data OR the processing activities require regular systematic monitoring of data subjects on a large scale (e.g. hospitals).
Consent – must have been freely given, be specific and informed	As before, but also consent must be clear, recorded, and be able to be withdrawn. Data Controllers must be able to demonstrate that consent has been given if consent is used as the basis for processing.
No legal obligation for data controllers to report breaches of security	Data breaches must be reported to supervisory authority (ICO in the UK) within 72 hours and in some cases to the data subjects as well.
Data Protection Impact Assessments are good practice for projects involving personal data	Data Protection Impact Assessments are now mandatory for projects/processing likely to result in a high risk to rights and freedoms of natural persons
Subject Access Requests – data to be provided to subject within 40 days and a fee of £10 could be charged	Subject Access Requests – data to be provided within one month and no fee chargeable. However, a 'reasonable fee' can be charged if the request is manifestly unfounded, excessive, or repetitive. A reasonable fee can also be charged to comply with requests for further copies of the same information. This does not mean that an organisation can charge for all subsequent access requests. Any reasonable fee must be based on the administrative cost of providing information.
Maximum penalty is £500,000	Maximum penalty could be up to €20 million or up to 4% of global turnover.
Accountability – limited and Data Processors have very little unless tied down in contract with a Data Controller	Data Controllers must be able to demonstrate that they comply with GDPR and there are requirements on Data Processors.

2 Community Chaplaincy Data Audit Example

DATA AUDIT		
DATA SET Clients files	Date 01/05/2018 Review date :	Auditor Emma Wells (data controller)
Referral forms Risk Assessments OASYS PNOMIS/other external paperwork Client/Mentor consent agreement Client privacy notice	Mentor meeting records Client Action Plan Referrals to other providers done with clients Case recording Case closure and outcome documents	Correspondence from external agencies about client Correspondence on behalf of client Eg help with covering letter for CV
DATA CONCERN	RESPONSE	ADDITIONAL ACTION
Where is it held ? physical and electronic?	*Client database on a Shared drive which is password protected* *Locked files in locked office*	*Ensure all staff understand the importance of keeping the sensitive data safe.*
Who has access to it and how is it accessed?	*Staff and one DBS checked admin volunteer* *Emails sent via CJSM if they are sensitive and contain sensitive data*	*Check all DBS are up to date*
Which system is it stored on? How is this safe	*Case notes are stored on a password protected database.* *The server is in a locked office. The external hard-drive back up is kept in a locked safe.* *Chaplaincy uses iizuka the CCA database*	*Contact CCA for their statement on the security of iizuka*
Who processes it and for what reasons?	*Staff members to update case progress* *Manager to access reports*	
Who is it disclosed to and for what reasons?	*Matched volunteer and probation officer MAPPA meeting for safeguarding and best delivery*	*Do we need to amend our Privacy Notice and send it to MAPPA ?*
What operational/technical measures are in place to uphold lawfulness?	*Leaflet in plain English for clients* *Staff explain process as they are doing assessments and seek ongoing consent and engagement with clients* *Clients have copies of Privacy Notice and Mentoring Agreement which clearly sets out the purpose of the work and the expectations both ways* *IT provider has been*	*Get explicit statement from our IT provider about how they uphold the security and the levels of safety/encryption*

	informed of sensitivity of work and built security accordingly	
What operational/technical measures are in place to uphold purpose limitation?	*The database is not designed to hold other irrelevant information* *Supervision process for staff and volunteers monitors interractions with volunteers and clients to ensure on task*	
What operational/technical measures are in place to uphold data minimisation?	*Database not designed to hold irrelevant information - Work is organised around pathways and goals which minimises the risk of unnecessary data being gathered Staff supervision includes sample viewing of case notes for safeguarding*	
What operational/technical measures are in place to uphold accuracy?	*Staff and volunteers check information back with clients and providers as accuracy on transfer is a recognised issue* *Clients have sight of their action plans and progress charts and can point out inaccuracies* *Clients are aware of Rectification procedures given in the privacy notice and who to contact if they cannot resolve inaccuracies with mentors or staff*	
What operational/technical measures are in place to uphold storage limitation?	*Currently none in place*	*Trustees to agree on a cut off for anonymising files.* *Trustees to decide date for destruction of physical case files* *Staff to implement*
What operational/technical measures are in place to uphold integrity and confidentiality?	*Clients are informed about the safe practices outlined above in terms of IT and physical security of data* *Clients are informed about their rights and staff and volunteers are trained on how to recognise requests for access rectification withdrawal etc.*	*Write policies on Access/Rectification/Erasure/ Portability/Ex automated Response Requests to include:* *How to recognise a request* *Verifying Identity* *Escalation procedure* *Managing timescales* *Handling rejections* *Ongoing relationship*

3 Sample Lawful Basis Assessment

DATA ITEM	PURPOSE	LAWFUL BASIS	COMMENT/ ACTION
Volunteer initial application form	Recruitment	Legitimate interest	May contain sensitive information
Volunteer completed interview questions and interviewers comments	Safeguarding and Project delivery	Legitimate interest	May contain sensitive information
Notes on volunteer suitability at training event	Safeguarding Project delivery	Legitimate interest	May contain sensitive information
Post training interview notes by chaplains	Safeguarding Project delivery	Legitimate interest	May contain sensitive information
Volunteer ICE information contact numbers etc	Project delivery Health and Safety	Legitimate interest	May contain sensitive information
Volunteer expenses forms	Project delivery	Legitimate interest	
Volunteers client pack containing client information	Project delivery	Contractual - mentors agreement	Enabled by previous obtained Consent from Client
Volunteer & client mentor agreement	Project delivery	Contractual	
Volunteer feedback notes on mentoring meetings in the community	Safeguarding Project delivery	Contractual (from mentors perspective) Public task or contractual (if sharing back with probation)	May contain sensitive information
Volunteer client chaplain supervision/review notes	Performance management safeguarding	Contractual	May contain sensitive information
Correspondence between volunteer and chaplain about client	Project delivery	Contractual (from mentors perspective) Public task or contractual (if sharing back with probation)	May contain sensitive information
Correspondence between staff and volunteer about volunteer	Performance management duty of care	Legitimate interest Consent	May contain sensitive information
Appraisal documents	Performance management	Legitimate interest	May contain sensitive information
Photos id cards	Project delivery	Legitimate Interest	
Appearing in a promotional video or photograph	Marketing publicity	Consent	

4 Sample Consent Agreement

CLIENT CONSENT AGREEMENT

To enable us to support you effectively, we may need to work with your Offender Manager and staff from other agencies. We will also need to store details of you on our secure database and store any information received in paper form. We understand that this information is sensitive. This information is kept in a secure office and on a secure computer. All data is stored under General Data Protection Regulations GDPR. If you have any problems regarding this please refer to your Privacy Notice and discuss with a member of staff.

I hereby give permission to Community Chaplaincy and all agencies indicated below to give and receive information about me, enabling Community Chaplaincy to work professionally alongside my Offender Manager and said agencies including the processing and safe storage of my information.

Agency *	✔
Offender Manager/Probation/Prison	
Substance Misuse Agencies	
Benefits Agency/Jobcentre Plus	
Social Worker/Social Services	
Employer/ Recruitment Agencies	
Education & Training Agencies	
Local Housing Providers	
GP	
Mental Health Services	

Signed_____

Printed Name_____

Date_____

*** if you tell us something that puts you someone else or a child at risk we will have to share the information.**

PRIVACY NOTICE

Date ……..

Dear ……..

This Community Chaplaincy is careful about personal data relating to you. This data may contain sensitive information about you such as your health, convictions, sexuality or religion.
We will hold your personal data following the principles below

You understand why your data is being processed
It will only be used for this purpose
It will be limited to what is necessary for the purpose
It will be up to date
It will not be kept in identifiable form for longer than is necessary
It will be held securely

You have the right to request at any time:

To be informed about what your data is being used for
To have access to your data within 30 days
To have any mistakes in your data corrected (within 30 days)
To have your data erased (if you withdraw your data we will not be able to work with you)
To 'port' your data to another provider
To object to how your data is processed
To have your data suspended (out of play) if a dispute is being processed
To have your data processed by a human not a computer

I am the nominated lead in the organisation for personal data. I can be contacted by emailing emmawells@communitychaplaincy.org.uk using the subject header GDPR also include here any other data processors (third parties) who will be processing the data on behalf of your organisation if that is the case

We will hold your personal data under the following lawful basis – Please tick

Legitimate Interest - to best provide you with the service you have requested
Contractual – We have a contract with you
Public Task - We have received your data in an official capacity from a provider such as probation
Consent – you have given us consent to have this data.

We will keep this information safely whilst you work with us and for one year afterwards, after which it will be anonymised so that it is no longer identifiable as you.

Kind regards

Emma Wells
Data Controller
Chaplaincy Name

GDPR SUBJECT ACCESS REQUEST (SAR) FORM

Name of Applicant …… Date of Request ……

Received by (name)……..

Position in organisation ……

Mode of request (email verbal etc) ……Request instance ……

REQUEST CATEGORY please tick

☐ ACCESS ☐ RECTIFICATION ☐ ERASURE ☐ PORTABILITY ☐ OBJECTION

Details……
……
……
……
……
……

ACTION CHECKLIST

Identity verified on …… by sight of ……accepted ID
signed by ……name……..

Application adjudicated by ……

position in organisation …… Date……..

OUTCOME ☐ REQUEST UPHELD ☐ REQUEST DECLINED Date ……

Applicant informed ☐ Date ……

Compliance action completed Date …… by ……

position in organisation ……

Comments……
……
……Case closed on
date……..

This is an example of the information necessary to record a data breach.

Identification Details *Organisation Name – is it the data controller? If not also add name of data controller* *Data controller's registration number* *Name/ job title/email of contact person for the breach*	
Summary of Breach *When and how you found out about the breach; Date location reporter.* *The people that have been or may be affected by the breach;* *What personal data has been placed at risk?* *How many individuals affected? Are they aware?* *What are the potential consequences?* *Have any affected people complained?* *Please specify if any financial or sensitive personal data has been affected and provide details of the extent*.	
Containment and Recovery * *What has been done to minimise/mitigate the effect on the affected individuals?* *Has the data placed at risk now been recovered? If so, please provide details of how and when this occurred what has happened.* *What you are doing as a result of the breach.*	
Policy and Procedure *Copy or location of Breach Procedure or policy being followed* *Flowchart or policy document with named contact individuals*	
Training and Guidance *Date of last DP training for staff members involved*	
Learning *Details of any procedure changed to reduce further risk (learning) May be added at a later date*	

**Serious breaches should be reported to the ICO using the DPA security breach helpline on 0303 123 1113 (open Monday to Friday, 9am to 5pm). Select option 3 to speak to staff who will record the breach, provide: a case reference number and give you advice about what to do next*