



Data Protection Policy and Privacy Notice - GDPR May 2018

Data Controller

Katie Dockery is the Data Controller under the Act, which means that they determine what purposes personal information held, will be used for. They are also responsible for notifying the Information Commissioner of the data Viewpoint Centre (VC) holds or is likely to hold, and the general purposes that this data will be used for. Information Commissioner notified 02.10.17
In case of any queries or questions in relation to this policy please contact Katie Dockery – info@viewpointcentre.org, 0300 772 9692

Introduction

VC needs to collect and use certain types of information about the Individuals who come into contact with VC in order to carry on our work. This personal information must be collected and dealt with appropriately, whether collected on paper, stored in a computer database, or recorded on other material and there are safeguards to ensure this under the law.

Any breaches of this Policy will be viewed very seriously. All personnel must read this policy carefully and make sure they are familiar with it. Breaching this policy is a disciplinary offence. The Data Protection Act 1998 (“DPA”) applies to any personal data that we process, and from 25th May 2018 this will be replaced by the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (“DPA 2018”), and PECR (together “Data Protection Laws”) and then after Brexit the UK will adopt laws equivalent to these Data Protection Laws.

In summary Data Protection laws (including GDPR) require that personal data is:

1. processed lawfully, fairly and in a transparent manner in relation to individuals;

2. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
3. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
4. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
5. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
6. processed 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.

This policy explains how we are ensuring that all of these principles are put into practice, and has extra detail to supplement our Privacy Notices.

Personal data is data that relates to a living individual who can be identified from that data (or from that data and other information in or likely to come into our possession). That living individual might be an employee, participant (service user), trustee, volunteer, donor, customer, prospective customer, supplier, contractor or contact, and that personal data might be written, oral or visual (e.g. CCTV).

We will only process personal data where we have identified a “lawful basis”. There are six available lawful bases for processing personal data. No single basis is better or more important than the others. In summary, the six lawful bases are:

1. Consent: the individual has given clear consent for us to process their personal data for a specific purpose.
2. Contract: the processing is necessary for a contract we have with the individual, or because they have asked us to take specific steps before entering into a contract.
3. Legal obligation: the processing is necessary for us to comply with the law (not including contractual obligations).
4. Vital interests: the processing is necessary to protect someone’s life.
5. Public task: the processing is necessary to perform a task in the public interest or for our official functions, and the task or function has a clear basis in law.

6. Legitimate interests: the processing is necessary for our 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.)

Special category data under Data Protection Laws is personal data relating to an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union activities, physical or mental health, genetic or biometric details, sexual life or details of criminal offences. We will only process **special category personal data** when we can demonstrate a lawful basis as above AND ensure that the individual has given their explicit consent to the processing OR that another of the following conditions has been met:

- the processing is necessary for the performance of our obligations under employment law;
- the processing is necessary to protect the vital interests of the data subject. The ICO has previously indicated that this condition is unlikely to be met other than in a life or death or other extreme situation;
- the processing relates to information manifestly made public by the data subject;
- the processing is necessary for the purpose of establishing, exercising or defending legal claims; or
- the processing is necessary for the purpose of preventative or occupational medicine or for the assessment of the working capacity of an employee.

Young people: where a child is below the age of 16 we will require consent from the person holding parental responsibility

Processing almost any action taken by us in respect of personal data will fall under the definition of "processing, including for example collection, modification, transfer, viewing, deleting, holding, backing up, archiving, retention, disclosure or destruction of personal data, including CCTV images.

Research: THC is a research-intensive organisation and as such we share data with researchers. Any time we refer to researchers in this document we mean people who are bone fide researchers within a University, or (in the case of student researchers) are under the supervision of a senior researcher. We only share personal data or special category data with researchers if we have explicit consent or we have anonymised the data. VC (Surrey hub) is not contributing to the research at this time.

Data Map

We have performed a data mapping exercise and determined key areas where consent must be obtained and where specific care is needed to protect certain data. This will be reviewed annually alongside this policy. Staff must make sure they use our Data Map in conjunction with this policy.

Our Data

The following records containing personal data and/or special category personal data may be held by VC as paper records and/or in digital form.

- Participant case notes (may include referral info, contact info, consent forms, external funding applications)
- Personnel records (may include application forms, contracts/agreements, training certificates, assessments, health records, financial info, DBS checks) for staff/volunteers/trustees
- Contracts (eg horse loan agreements)
- Compliance records (may include complaints, reports of safeguarding concerns, accident, incident, or near miss reports)
- Address Book (may include personal data for donors, supporters, personnel, contracting parties, professionals)

Data sharing/processing

We may share data with other agencies such as:

- The local authority
- NHS
- Schools/Colleges
- VSO service providers
- Police, probation
- HSE, RIDDOR
- Safeguarding Board / MASH
- Researchers
- Funding bodies (rarely)

We will always be mindful of the rights and interests of the data subject and make sure the sharing is appropriate and proportionate. Sharing or processing of data will be on the basis of one of the six principles outlined above, depending on the data and task.

Below we give examples of how we have applied the principles to our data flow through our Data Map.

1. Consent
2. Contract
3. Legal obligation
4. Vital interests
5. Public task
6. Legitimate interests

1. Consent

Whenever we hold or share *special category* data we will rely on explicit opt-in consent. When we receive referrals we will only hold that data until our first contact with the participant, at which time we will ask for appropriate consents.

Eg. Receiving and sharing data about participants mental health with referrers

Sharing data for research purposes which might include offending, mental health data

Collecting personnel recruitment data which could include special category data (trustees, staff, volunteers).

Whenever we process *personal data* we will rely on explicit opt-in consent unless we have another lawful basis. We will ask for consent before:

Eg. contacting participants for follow up / research
sending participant video footage for external assessment
using photos/video for marketing purposes

2. Contract

We will process personal data for people where it is an essential part of a contract.

Eg. Staff
Contractors
Suppliers

3. Legal Obligation

We will process or share data where we are obliged to by law.

Eg. criminal prosecution, safeguarding concerns.

4. Vital Interest

We will process personal data if required to protect someone's life.

Eg. Handover to a medical professional in an emergency

5. Public task

Where we receive referrals from NHS or Local Authority we will either:

- Sign a joint processing agreement to cover our processing activities; or
- we will seek consent from participants to process their data upon first contact.

6. Legitimate interest

We will hold and process data such as contact details for referrees, supporters, donors and our existing supporter contacts under the basis of legitimate interest.

For each activity using this data we will consider three elements to the legitimate interests basis.

- What is our legitimate interest?
- Eg. To email referrers occasionally with updates to our services To email supporters with updates of our charitable activities
- Is the processing necessary and proportionate to achieve it?
- Eg. If there is a less intrusive way, we will do that
- We balance our legitimate interest against the individual's interests, rights and freedoms, If they would not reasonably expect the processing, or if it would cause unjustified harm, their interests will override ours.
- Eg. We are careful not to over-communicate, or to be too demanding of our supporters
- We never have and will never buy or sell contact lists
- We will always provide simple and prominent opt-out in our fundraising
- or promotional communications

We keep a record of our legitimate interests assessment (LIA) in our Data Map.

Data security

Our standard measures to protect personal data and special category personal data from data breach

- We maintain a Data Map – detailing data streams, risks and mitigations, reviewed annually
- We maintain a register of devices being used to process VC data, audited annually
- We maintain a register of Cloud services, audited annually to ensure they are GDPR compliant
- We maintain a register of devices such as computers, laptops, smart phones, including any personal devices used by staff in the course of their work. We check annually that they are properly protected and compliant with our GDPR responsibilities
- Locked filing cabinets for paper records, HDs, DVDs
- Key cabinet with combination lock
- Shredder for redundant paper records
- Data Protection training for all personnel, refreshed annually
- Safer recruitment policy to ensure appropriate personnel
- DBS checks to ensure appropriate personnel
- Safeguarding Training for all personnel, according to level of participant contact
- We use ‘explicit opt-in consent’ declarations and privacy notices for various data processing tasks, especially regarding special category data and in relation to all participant data.
- Participant data is frequently received in a referral from professionals in mental health, social services, schools or specialist support organisations. In this case we ask for assurances from the referrer that they have consent or other lawful use to share this data with us, and upon first contact (or via the referrer) we ask participants for ‘explicit opt-in consent’ for various data processing tasks.

Personal devices such as computers, laptops and smart phones used by personnel of VC to assist them in their work must be listed on the VC IT Register and managed by them to protect any information or data held relating to VC.

The following are protection measures all personnel of VC must take to protect data:

- All personal devices capable of accessing VC data MUST be password protected and should always be in a ‘locked’ mode when unattended.
- Use a separate password for any VC accounts (recommended minimum 8 characters, mix upper and lower case letters, use at least 1 number or punctuation)
- Never share your VC account passwords
- No VC personal data may be stored on the device itself - use the cloud services listed on our IT Register. Do not use personal devices to take videos/photos of VC subjects - use our designated devices and SD cards
- Process and back up photos/videos to a secure VC cloud/storage within 2 weeks, then delete any photos or videos from cameras and video cameras storage cards
- Take care to secure cameras and cards
- Take care with all personal data and items containing personal data you handle or come across so that it stays secure and is only available to or accessed by authorised individuals
- Immediately notify the VC Data Controller if you become aware of or suspect the loss of any personal data or any item containing personal data

- Immediately notify the VC Data Controller if any individual says or does anything which gives the appearance of them wanting to invoke any rights in relation to personal data relating to them
- You should always take a common sense approach, and if you see any areas of risk that you think are not addressed then please bring it to the attention of the VC Data Controller

Special measures to protect specific data include:

- We use encrypted email systems or anonymising whenever possible for communications pertaining to special category personal data, or any participant data – or secure internal messaging when a staff-only communication
- Data processing agreement to cover subcontracting payroll and pensions processing to our accountants
- Participant contact info (and that of carers) to be stored securely with casenotes – and only added to our supporter / donor contacts if consent is given

International transfers

We do not transfer personal data internationally. We check our cloud service providers to ensure they are GDPR compliant, including the transfer of data outside the EU.

Retention of data

VC will retain personal data as determined by our data map, in summary:

Participant case notes will be stored for 5 years in case they return for further services, data will then be anonymised and held for 10 years for research purposes. Where participants have given specific consent their data will not be anonymised, allowing for further contact and longitudinal studies. This is unusual and is because ours is an innovative methodology which attracts extensive research interest, also because research is one of our organisational priorities. Where participant data is received from our hubs we request that it is anonymised prior to sending to us.

Personnel data (trustees, staff, volunteers, approved facilitators, hub managers) or parties to contracts: financial data will be deleted as soon as it is no longer needed, remaining data (with the exception of a skeleton record including name and brief notes) after 3 years unless there are statutory obligations to retain specific data (eg safeguarding concerns).

Supporters, donors: we will communicate regularly but thoughtfully and always have an opt out option. We will not delete contacts simply on the basis of age as many supporters do not respond for many years whilst still remaining interested.

Public: We will not store contact details without consent or legitimate interest (based on prior contact). We will always have simple and prominent opt-out options. We will not buy or sell contact lists.

Accident/Incident/Complaint records will be anonymized wherever we can and deleted after 3years

Sign in registers will be kept for a period of 1 year for the purpose of recording staff and volunteer statistics and then destroyed

Safeguarding reports and records will be stored for 7 years before being deleted or destroyed under NSPCC guidelines

Text reminder service: Telephone number and name are stored for a maximum period of 1 year and not used for any other purpose

Photos and Videos will be stored indefinitely where we have explicit media consent from the subject. We will delete these records after 5yrs in all other cases

Our measures to prevent inappropriate retention of data and unwanted communications

- We will undertake a data check and purge to be completed by the end of 2018 or sooner, in response to our data mapping exercise
- Verbal/written consent to make contact for fundraising/marketing purposes will be recorded for all new contacts
- All marketing or fundraising communications will include a privacy notice and an opt out option
- We will amend or erase contact details if requested and will include easy, obvious opt-out buttons on any electronic 'marketing' materials.

Data subject rights

Under Data Protection Laws individuals have certain rights in relation to their own personal data.

In summary these are:

- Right to be informed including privacy information, including retention periods
- The right to access their personal data, usually referred to as a subject access request
- The right to have their personal data rectified
- The right to have their personal data erased, usually referred to as the right to be forgotten
- The right to restrict processing of their personal data
- The right to portability of their personal data
- The right to not be subject to a decision made solely by automated data processing (we do not do this)
- The right to object to receiving direct marketing materials

We respect these rights and take appropriate steps to satisfy them.

The exercise of these rights may be made in writing, including email, and also verbally – these are called Subject access requests (SAR).

The procedure for a SAR will be followed as detailed in the Information Commissioner’s Office (ICO) subject access code of practice.

<https://ico.org.uk/media/for-organisations/documents/2014223/subject-access-code-of-practice.pdf>

The ICO Subject Access Online Checklist will be used in each case of receiving a SAR:

<https://ico.org.uk/for-organisations/subject-access-request-checklist/>

Data Breach

Any data breach will be reported to the ICO within 72 hours of the breach

<https://ico.org.uk/for-organisations/report-a-breach/>

In the case of a high risk breach (e.g. criminal activity such as fraud, or published in the public domain) to the rights and freedoms of individuals then THC will notify those concerned without undue delay.

PECR

To comply with PECR we have adopted the ICO checklist.

- We only text or email “marketing” information with opt-in consent (unless contacting previous supporters about our own similar products, and we offered them an opt-out when they gave their details)
- We offer an opt-out (by reply or unsubscribe link)
- We keep a list of anyone who opts out
- We screen against our opt-out list

Updates

This policy will be updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments made to Data Protection laws.

Date updated	Updated by	Due for review
05/2018	KD, EW	12/2018 to ensure all proposed purging of historical data is complete