

Data Protection, Privacy and Confidentiality Policy

Contents

1. Introduction	2
2. Purpose of the policy	2
3. How we use your information	3
4. Sharing your information.....	3
5. Data security	4
6. How long we keep your information.....	4
7. Access to your own information.....	4
8. Removal of your information	5
9. Verification of your information.....	5
10. Queries and complaints.....	5
Appendix 1 The reasons we collect your information	6
Appendix 2: Personal Data Breach	11
Appendix I: Personal Data Breach Record Form.....	19
Appendix II: Personal Data Breach Risk Assessment Checklist	21
Appendix III: Guidance relating to notification of personal data breaches	22
Appendix 3: Managing Vulnerable Clients' Data	24

Associated policies and procedures

Safeguarding Adults	Clear Desk Policy
Communications, Use of IT and Telephony	Digital Safeguarding Policy
DBS Disclosure Policy	Equity, Diversity, Inclusion and Belonging Policy
Disciplinary Policy and Procedure	Fundraising Pledge
Fundraising and Communications Data Protection and Privacy	Recruitment, Selection and References Policy
Grievance Policy and Procedure	Service Charter
Safeguarding Children and Young People	Complaints Policy and Procedure
Serious Incident Reporting Policy	Unacceptable Behaviour by Service \users and Third Parties Policy
Social Media and Attributed Digital Content Policy	Working with Suicidal Service Users Guide
Whistleblowing (Public Interest Disclosure) Policy	Data Retention Policy

If you have any question regarding this policy, please contact our Director of Administration and Corporate Services kevans@ch1889.org or the Chief Executive kwoodley@ch1889.org the designated Data Protection Officers

1. Introduction

- a) Cambridge House pursues a vision of a society without poverty where all people are valued, treated equally and lead fulfilling and productive lives.
- b) We are an independent social action charity that works to tackle poverty and promote social justice:
 - Company limited by guarantee no.105006 and registered charity no.265103.
 - Address: Cambridge House, Unit F, Ground Floor, The Print Works, 22 Amelia Street London SE17 3PY
- c) This Data Protection, Privacy and Confidentiality Policy tells you what to expect regarding the personal information collected and processed by Cambridge House.
- d) We offer a wide variety of different services to local communities, children and young people, families, adults, charities and community groups, statutory agencies, private businesses and general members of the public.
- e) Everything we do, we do to ensure that we can help our service users get both support and respect. We want to make sure you receive the communications that are most relevant to you, be it through visiting our website or receiving emails, post or phone calls. We want to make sure you receive the best attention when you use our services, become a member, join our team of volunteers and employees or donate.
- f) We primarily collect information from you through direct contact. This could be if you ask us about our activities, request our support, donate to us, ask a question about a service, apply for a job or volunteering opportunity or otherwise provide us with your personal information. This includes when you phone us, visit our website or get in touch through the post, or in person.
- g) We have a separate [Fundraising and Communications Data Protection and Privacy Policy](#) which you can find on in our Teams Staff Policy and Procedures folder.

2. Purpose of the policy

- a) This policy sets out how we will collect, process, store, use and protect the privacy and confidentiality of the information we hold about you.
- b) We take seriously the protection of your privacy and confidentiality and we understand that you are entitled to know that your personal data will not be used for any unintended purpose and will not accidentally fall into the hands of a third party.
- c) We undertake to preserve the confidentiality of all information you provide to us.
- d) Our policy complies with UK law accordingly implemented, including that required by the EU General Data Protection Regulation (GDPR).
- e) The law requires us to tell you about your rights and our obligations to you regarding the processing and control of your personal data. This information can be found at www.knowyourprivacyrights.org
- f) Except as set out below, we do not share, or sell, or disclose to a third party, any information personal information we collect.

3. How we use your information

- a) We only ever use your personal data if we are satisfied that it is lawful and fair to do so because:
 - You have given your consent to us using your information for the specific purposes described in this privacy notice
 - It is necessary to enter into, or perform, a contract with you in order to comply with a legal obligation for our own (or a third party's) legitimate interests provided your rights don't override these interests. For example, we may use your personal data to:
 - Comply with fraud and crime protection and for our network and information security measures
 - Fulfil our obligations as defined by law or our regulatory authorities
 - Identify usage trends and for data analytics as this information will help us review and improve our services
 - Provide you with information that we have a reasonable expectation you would expect to receive or that would benefit and enhance our relationship.
- b) We will only use special categories of personal data relating to you or to third parties you tell us about when we have your explicit consent and/or where it is necessary to use the information for the establishment, exercise or defence of legal claims.
- c) We will never sell your personal data or share it with third parties who might use it for their own purposes.
- d) **Appendix 1** provides more detail on:
 - The reasons we collect information
 - What information we need
 - Why we need the information

4. Sharing your information

- a) The personal information we collect about you will mainly be used by our staff (and volunteers) so that they can support you.
- b) We will never sell or share your personal information with organisations so that they can contact you for any marketing activities.
- c) We will never sell any information about your web browsing activity.
- d) We will not disclose any information you provide to any third parties other than:
 - Where you have given us consent to share the information
 - Where we instruct professional advisors on your behalf (for example, barristers, medical professionals or other experts) where necessary to carry out your request for support
 - If we are under a legal or regulatory duty to disclose or share your personal information (for example, if required to do so by a court order or for the purposes of prevention of fraud or other crime or in relation to audits, enquiries or investigations by regulatory bodies)
 - To enforce any terms and conditions or agreements between us as part of a sale of some or all our business and assets to any third party or as part of any business restructuring or reorganisation (we will always notify you in advance and we will aim to ensure that your privacy rights will continue to be protected)

- To protect our rights, property and safety, or the rights, property and safety of others (this includes exchanging information with our insurers, other companies, organisations and regulators for the purposes of fraud protection and credit risk reduction)
 - Anonymised for the purposes of research and quality assurance.
- e) We may share results of research that we carry out into the use of our services with third parties, but this information will always be anonymised and will not contain your personal information.

5. Data security

1. We take looking after your information very seriously. We've implemented appropriate physical, technical and organisational measures to protect the personal information we have under our control, both on and off-line, from improper access, use, alteration, destruction and loss.
2. Unfortunately, the transmission of information using the internet is not completely secure. Although we do our best to protect your personal information sent to us this way, we cannot guarantee the security of data transmitted to our site.
3. Our websites may contain links to other sites. While we try to link only to sites that share our high standards and respect for privacy, we are not responsible for the content or the privacy practices employed by other sites. Please be aware that:
 - Web sites that have links on our site may collect personally identifiable information about you. This privacy statement does not cover the information practices of those websites or advertisers.

6. How long we keep your information

- a) We will keep your details on record for as long as it is reasonable and necessary for the relevant service or activity, or as is set out in any contract we hold with you and then for a period afterwards, to be determined by applicable legislation, regulations and best practice.
- b) Unless otherwise specified by law or a regulatory authority; our default retention period for personal data, is seven years from the conclusion of your relationship with us.
- c) This enables us to:
 - Provide you with the services you have requested. This includes a record of the services and or support you have used at Cambridge House so that we can provide the best possible service should you contact us in the future.
 - Support a claim or defence in court.

7. Access to your own information

- a) You may obtain a copy of any information we hold about you by sending us a request at data@ch1889.org
- b) After receiving the request, we will tell you when we expect to provide you with the information, and whether we require any fee for providing it to you.

8. Removal of your information

- a) If you wish us to remove personally identifiable information from our systems, you may contact us at data@ch1889.org
- b) This may limit the service we can provide to you.

9. Verification of your information

- a) If you wish to edit or delete personal identifiable information, you may contact us at data@ch1889.org
- b) When we receive any request to access, edit or delete personal identifiable information we shall first take reasonable steps to verify your identity before granting you access or otherwise taking any action. This is important to safeguard your information.

10. Queries and complaints

- a) Our Director of Administration and Corporate Services oversees compliance with this privacy notice. If you have any questions about this privacy notice or how we handle your personal information, please contact feedback@ch1889.org
- b) You have the right to make a complaint at any time to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues.

Appendix 1 The reasons we collect your information

Reasons we collect information	What information we need	Why we need the information
For the provision of services to the people who have requested them		
Safer Renting and Independent Advocacy services	<ol style="list-style-type: none"> 1. We will collect personal information about you when you contact us about providing advice and or advocacy services to you (for example, your name, address, email contact details, telephone number). 2. While providing advocacy and advice services to you, we may collect information about you and/or any other individuals you tell us about. 3. Depending on the nature of the work we carry out for you, we may collect and use special categories of personal data about you or a third party you tell us about (for example, information about health, special educational needs, ethnic origin, religious or philosophical beliefs). 	<p>We collect the information about you so that we can:</p> <ol style="list-style-type: none"> 1. Provide you with the information or services that you have requested from us and for other closely related purposes. 2. To provide you with information about our work or our activities where you have agreed to receive communications from us. 3. Comply with regulatory requirements. 4. Aggregate this information in a general way and use it to provide quality assurance information and research data, for example to monitor our performance with respect to a service we provide. <p>If we use it for this purpose:</p> <ul style="list-style-type: none"> ▪ You as an individual will not be personally identifiable. ▪ It will enable us to improve the quality of the services we offer.
Law Centre	<ol style="list-style-type: none"> 1. We will collect personal information about you when you contact us about providing legal services to you (for example, your name, address, email contact details, telephone number). 2. While providing legal advice services to you, we may collect information about you and/or any other individuals you tell us about. Depending on the nature of the work we carry out for you, we may collect and use special categories of personal data about you or a third party you tell us about (for example, information about health, ethnic origin, religious or philosophical beliefs, and/or trade union membership). 3. We will only use special categories of personal data relating to you or to third parties you tell us about when we have your explicit consent and/or where it is necessary to use the 	

	information for the establishment, exercise or defence of legal claims.	
Education and inclusion services (Disabled Peoples' Empowerment and Youth Empowerment)	<ol style="list-style-type: none"> 1. We will collect personal information about you when you join a disabled peoples' or young peoples' education and empowerment project (for example, your name, address, email contact details, telephone number). 2. Once you have enrolled on a project, we may collect information about you and/or any other individuals you tell us about (for example, your parents or carers and or an emergency contact). 3. Depending on the nature of the project you join, we may collect and use special categories of personal data about you or a third party you tell us about (for example, information about health, educational needs, ethnic origin and/or religious or philosophical beliefs). 	
Office and venue hirers	<ol style="list-style-type: none"> 1. We will collect personal information about you when you contact us about providing office or venue hire spaces to you (for example, your name, address, email contact details, telephone number). 2. Once you have decided you want us to provide you with office or venue hire space, we may require further information before entering into a license or contract legal with you (for example, insurance, references and or company accounts) to comply with our due diligence requirements. We may also collect data about you from publicly accessible sources, e.g. Companies House or the Charities Commission 	
If you have a query or a complaint		
<ol style="list-style-type: none"> 1. Name and contact details 2. Description of query or complaint (including identity of any other individuals involved in the complaint) 		To process the query or complaint and to check on the level of services we provide.

To fulfil our responsibilities as an employer		
Current and former employees and volunteers	<ol style="list-style-type: none"> 1. Your application form and references 2. Your contract of employment and any amendments to it 3. Correspondence with or about you (for example, a letter to your mortgage provider to confirm your salary) 4. Information needed for payroll, benefits and expenses purposes 5. Contact and emergency contact details 6. Records of holiday, sickness and other absence 7. Information for equal opportunities monitoring 8. Records relating to your career history (for example, training records, appraisal, disciplinary and grievance records, reasonable adjustment agreements) 9. Information about your health 	<ol style="list-style-type: none"> 1. To enable us to comply with the employment contract, to comply with any legal requirements, pursue the legitimate interests of the company and protect our legal position in the event of legal proceedings. 2. To comply with our health and safety and occupational health obligations
If you apply to us for a paid or voluntary position	<ol style="list-style-type: none"> 1. Name and contact details 2. Your referees 3. Your previous experience, education and qualifications gained 4. Answers to questions relevant to the role you have applied for 5. Equal opportunities information 6. You will be asked to complete a criminal records declaration to declare any unspent convictions 	<ol style="list-style-type: none"> 1. We will use the contact information to contact you to progress your application. 2. If we make you a conditional offer of employment we will contact your referees to obtain references. 3. We will use the other information to assess your suitability for the role you have applied for. 4. The equal opportunities information is not mandatory. Any information you do provide, will be used only to produce and monitor equal opportunities statistics and these will not be presented in a way that can identify you. If you supply this information, it will be separated from your application and will not form part of the recruitment process in any way.

<p>If we make you a conditional offer of employment or a position as volunteer, trainee or intern</p>	<ol style="list-style-type: none"> 1. Proof of your identity 2. Proof of qualifications 3. Information required to complete a request for the Disclosure and Barring Service. 4. We may (dependent upon role) ask you to complete an Employment Capability Declaration questionnaire about your health. 	<ol style="list-style-type: none"> 1. If we make a conditional offer of employment, we will ask you for information so that we can carry out pre-employment checks. 2. You must successfully complete pre-employment checks to progress to a confirmed, unconditional offer. 3. We are required to confirm the identity of our staff, their right to work in the United Kingdom and seek assurance as to their trustworthiness, integrity and reliability.
<p>If we confirm an offer of employment or a position as volunteer, trainee or intern</p>	<ol style="list-style-type: none"> 1. Bank details 2. HMRC and Payroll Starter Checklist 3. Emergency contact and medical information (for example, allergies to penicillin) 	<ol style="list-style-type: none"> 1. To process salary payments 2. To ensure you are placed on the right tax code and to capture student loan data where applicable 3. So that we know who to contact in case you have an emergency at work 4. So that we can inform emergency services of any specific medical conditions that may be relevant to your care
<p>If you provide a reference for an applicant for a job or a position as volunteer, trainee or intern</p>	<ol style="list-style-type: none"> 1. Name and contact details 2. Relationship to the applicant 	<p>To contact you to carry out pre-employment checks for someone who has applied to us for a job or a position as volunteer, trainee or intern</p>
<p>If you are a member or patron</p>		
<ol style="list-style-type: none"> 1. Name, address, telephone number and email address 2. Records of our communications and interactions with you (for example, notes of our meetings with you; records of which of our events you have attended, email exchanges between us) 3. If you attend one of our events <ul style="list-style-type: none"> ▪ Dietary requirements ▪ Accessibility requirements 		<ol style="list-style-type: none"> 1. For our legitimate business interests of working to tackle poverty and promote social justice. 2. To meet the requirements of Charity and Company Law. 3. To comply with the requirements of our articles of association.

If you visit our website	
<ol style="list-style-type: none"> 1. We will collect personal information that you voluntarily provide to us if you fill in a form on our website or apply for a vacancy through the website. <ul style="list-style-type: none"> ▪ This information may include your contact details including name, address, email, telephone number and where you provide it, some categories of personal data for example, ethnic origin and religious beliefs. 2. Information we collect using cookies and similar technologies: <ul style="list-style-type: none"> ▪ Your device's location (IP address) ▪ Referring website ▪ Visits, which may include traffic data ▪ Pages visited ▪ Time visited our website ▪ Information about your Internet service provider ▪ Your operating system ▪ Browser type 	<ol style="list-style-type: none"> 4. To keep you up to date with our work and activities, publications, blogs, events, job vacancies and to respond to your enquiries 5. To provide you with a better experience on our site, for administration and reporting purposes (for example, for troubleshooting) and to find out which parts of the site are popular
If we send you updates on our research, invite you to our events, or invite you to engage with us in other ways	
<ol style="list-style-type: none"> 1. Name, Email address and if appropriate Job title and Organisation 2. Records of our communications and interactions with you (for example, notes of our meetings with you; records of which of our events you have attended, email exchanges between us) 3. If you attend one of our events <ul style="list-style-type: none"> ▪ Dietary requirements ▪ Accessibility requirements 	For our legitimate business interests of working to tackle poverty and promote social justice.
If you are one of our suppliers (including consultants and contractors)	
<ol style="list-style-type: none"> 1. Name 2. Address 3. Email address 4. Telephone number 5. Bank details 6. Safeguarding, equalities, insurance, GDPR and legal compliance information 	To help us when we are considering purchasing a service or negotiating a contract with you and where you may act as a supplier.

Appendix 2: Personal Data Breach

Contents

1. Statement.....	12
2. What is a personal data breach?	12
3. What must you do in the event of a personal data breach?.....	13
4. Who is responsible for dealing with data breaches	14
5. Five-Step process for managing of personal data breaches	14
6. Is legal advice needed?	18
7. Reviewing this policy	18
8. Retention of documents.....	18
APPENDIX 2a: Personal Data Breach Record Form.....	19
APPENDIX 2b: Personal Data Breach Risk Assessment Checklist.....	21
APPENDIX 2c: Guidance relating to notification of personal data breaches.....	22

1. Statement

- a) The General Data Protection Regulation ('GDPR') introduces mandatory obligations on organisations which process and exercise control over personal data (known as "controllers") to notify personal data breaches to the relevant supervisory authority (for our purposes, this will usually be the Information Commissioner's Office ("ICO")) and individual data subjects.
- b) Cambridge House is a controller under the GDPR and is, therefore, subject to these mandatory breach notification obligations.
- c) Failure to notify personal data breaches to relevant supervisory authorities and data subjects in accordance with the requirements of the GDPR may lead to Cambridge House receiving financial fines.
- d) Whilst we take the safety and security of the personal data that we process extremely seriously and have in place technical and organisational measures designed to protect the security of personal data, it is not possible to eradicate entirely the risk of a personal data breach.
- e) The purpose of this procedure is, therefore, to set out how we will deal with a personal data breach under the GDPR. Adhering to this procedure will help ensure that:
 - i) personal data breaches are dealt with appropriately, effectively and efficiently; and
 - ii) we meet the requirements of the GDPR.
- f) All trustees, members of staff, volunteers, interns and contractors are required to familiarise themselves with and follow the procedures set out in this document.
- g) In view of the potentially serious consequences (both for data subjects and Cambridge House) that may flow from failing to notify a personal data breach in accordance with the requirements of the GDPR, we require all trustees, members of staff, volunteers, interns and contractors to act responsibly and quickly if they become aware of a personal data breach. Failing to do so, may amount to a disciplinary offence

2. What is a personal data breach?

- a) A personal data breach is legally defined as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed".
- b) You can find out more information about what constitutes personal data by looking at our Data Protection and Privacy Policy.
- c) The following are all examples of personal data breaches:
 - i) personal data is accidentally lost or deleted by an employee;
 - ii) personal data is corrupted;
 - iii) someone accesses personal data or passes it on without proper authorisation;
 - iv) there is a network intrusion by a third party (e.g. a hacking incident or another type of cyber security attack);
 - v) data or equipment on which personal data is stored, is lost or stolen;

- vi) inadequate security controls (such as weak passwords) result in an unauthorised person gaining access to an IT system which includes personal data;
- vii) human error resulting in information being sent to the incorrect recipient;
- viii) personal data is destroyed by unforeseen circumstances such as fire or flood;
- ix) a 'blagging' offence takes place where information is obtained by deception.

3. What must you do in the event of a personal data breach?

a) Notification to the ICO and/or data subjects

- i) If there is a personal data breach:
 - there is a requirement to notify the ICO unless the breach is unlikely to result in a risk to the rights and freedoms of individuals; and
 - there is a requirement to notify individual data subjects where the personal data breach is likely to result in a high risk to the rights and freedoms of individuals.

b) Timescales

- i) **Notifying the ICO**
 - Where a personal data breach requires notification to the ICO, the GDPR requires that this takes place without undue delay and, where feasible, no later than 72 hours after we become aware of the personal data breach.
 - The clock starts ticking from the time we have enough information to confirm that there has been a breach and provide some basic facts. This is the case even if it is not possible to provide full details now. Additional information may be provided to the ICO in stages provided this is done without undue further delay.
 - If the initial notification is not made within 72 hours, it is necessary to inform the ICO of the reasons for the delay in reporting the breach.
- ii) **Notifying individual data subjects**
 - Where a personal data breach requires notification to individual data subjects, the GDPR requires that this takes place without undue delay. Whilst there is no overall deadline, communications to data subjects should be made as soon as reasonably feasible and in close co-operation with the ICO.

c) Keeping a record of personal data breaches

- i) Irrespective of whether there is a duty to notify the ICO or individual data subjects, the GDPR requires us to keep a record of personal data breaches.
- ii) The record must include:
 - the facts relating to the breach;
 - the effect of the breach;
 - confirmation of any remedial action taken
- iii) The ICO may require sight of the record to verify we have complied with the GDPR.

4. Who is responsible for dealing with data breaches?

- a) Our Director of Administration and Corporate Services and Chief Executive are designated Data Protection Officers responsible for ensuring that personal data breaches are dealt with efficiently and effectively, including:
 - i) assessing and containing any personal data breach;
 - ii) investigating the breach;
 - iii) ensuring the GDPR's record keeping requirements are met;
 - iv) making any necessary notifications under the GDPR;
 - v) evaluating lessons learned; and
 - vi) implementing any additional security or procedural measures deemed necessary to minimise the risk of a similar personal data breach occurring and/or to improve our methods of handling personal data breaches
- b) The Director of Administration and Corporate Services may require the assistance of members of staff. For example, those who are involved in a personal data breach and/or who have the expertise necessary to assist with the containment, assessment, evaluation of or recovery from a personal data breach.
- c) In the absence of the Director of Administration and Corporate Services, the Chief Executive is responsible for ensuring that personal data breaches are dealt with efficiently and effectively.
- d) All personal data breaches will be reported to the Board of Trustee's Company Secretary (who is also the Chief Executive).

5. Five-Step process for managing personal data breaches

- a) **Step 1 – The logging of a personal data breach**
 - i) Upon becoming aware of any personal data breach, a member of staff must take immediate action to bring the breach to the attention of the Director of Administration and Corporate Services (or, in their absence, the Chief Executive) in person or by telephone.
 - During working hours, you should use the relevant person's extension number or work mobile number.
 - Outside normal working hours you should use their work mobile number.
 - All personal data breaches must be reported in this way by anyone who becomes aware of a personal data breach. It is not for members of staff to assess and determine the potential seriousness of any personal data breach. That is the role of the Director of Administration and Corporate Services (or in their absence the Chief Executive).
 - ii) Immediately after the member of staff has brought the personal data breach to the attention of Director of Administration and Corporate Services (or in their absence the Chief Executive); the member of staff must officially log the breach by filling out Part 1 of the Personal Data Breach Record Form set out in Appendix 1 of this Policy, and emailing the form to Director of Administration and Corporate Services (or in their absence the Chief Executive).

- iii) Director of Administration and Corporate Services (or in their absence the Chief Executive) will be responsible for completing Part 2 of the Personal Data Breach Record Form in due course, with the assistance of the member of staff who logged the breach if necessary.
 - The completed Personal Data Breach Record Form forms the basis of Cambridge House's compliance with the requirement under the GDPR that organisations keep records of all personal data breaches.
 - Director of Administration and Corporate Services (or in their absence the Chief Executive) will be responsible for filing the record in a dedicated corporate services file.
- iv) All correspondence or other documentation relating to the breach should be retained and passed to Director of Administration and Corporate Services (or in their absence the Chief Executive).

b) Step 2 - Containment and recovery of data

- i) Once the Director of Administration and Corporate Services (or in their absence the Chief Executive) has been made aware of a data security breach; they will:
 - identify who within Cambridge House needs to be made aware of the breach and inform them of what they are expected to do to assist in the containment exercise;
 - identify and implement, with the assistance of other members of staff as appropriate, the steps that need to be taken to contain the breach. Including, for example, remotely wiping a laptop or mobile telephone, isolating or closing a compromised section of the computer network, retrieving a lost piece of equipment or changing passwords and/or access codes;
 - establish whether anything can be done to recover any loss of data or to limit the damage the breach may cause;
 - determine whether police and/or our insurers should be notified of the personal data breach and, if deemed appropriate, make such notification.

c) Step 3 - Assessing the risks

- i) The next step that will be taken by the Director of Administration and Corporate Services (or in their absence the Chief Executive) is to assess the level of risk to the rights and freedoms of individuals that is likely to result from the breach for the purposes of:
 - determining whether the breach should be notified to the ICO and/or individual data subjects;
 - notifying any other regulatory bodies as appropriate; and
 - determining what other steps need to be taken to deal with the personal data breach.
- ii) This will require an assessment of the potential adverse consequences of the personal data breach for individuals. For example:
 - some personal data security breaches will not lead to risks beyond possible inconvenience to those who need the data to do their job and will not, therefore,

require notification to the ICO or individuals. For example, where a laptop is damaged, but its files were backed up and can be recovered, albeit at some cost to the business;

- other types of incidents may lead to significant risks. For example, the theft of a customer database which may be used to commit identity fraud.

iii) To assess the risks posed by a personal data breach and decide the appropriate response; the Director of Administration and Corporate Services (or in their absence the Chief Executive) will:

- complete the Risk Assessment Checklist set out in Appendix 2
- comply with the timescales relating to the notification of personal data breaches; and
- comply with the guidelines relating to when notifications may need to be made to the ICO or individual data subjects set out in Appendix 3 (the “Notification Guidelines”)

d) Step 4 - Notification of a personal data breach

- i) The ICO must be notified of any personal data breach unless it is unlikely to result in a risk to the rights and freedoms of individuals.
- ii) Individual data subjects must be notified of any personal data breach where the breach is likely to result in a high risk to the rights and freedoms of individuals.
- iii) Completion of the Risk Assessment Checklist and reference to the Notification Guidelines will assist the Director of Administration and Corporate Services (or in their absence the Chief Executive) to decide whether a personal data breach does or does not need to be notified to the ICO and individual data subjects.

iv) Notifying the ICO

Where the Director of Administration and Corporate Services (or in their absence the Chief Executive) concludes that a personal data breach requires notification to the ICO; they will ensure that the timing of the notification meets the ICO’s requirements, and the information provided includes the minimum information required by the GDPR, which is as follows:

- the nature of the personal data breach including, where possible, the categories and approximate number of data subjects and personal data records concerned;
- the name and contact details of the [Data Protection Officer/other];
- the likely consequences of the personal data breach;
- the measures taken or proposed to be taken to address the personal data breach, including any measures to mitigate its possible adverse effects.

v) Notifying individual data subjects

- Certain exceptions apply to the mandatory obligation to notify personal data breaches to individual data subjects. These are:
 - if the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular, those that render the personal data unintelligible to any person who is not authorised to access it,

- such as encryption;
 - if the controller has taken subsequent measures to ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialise;
 - if notification would require disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.
 - The Director of Administration and Corporate Services (or in their absence the Chief Executive) will determine whether an exemption relating to the notification of individual data subjects applies.
 - Where the Director of Administration and Corporate Services (or in their absence the Chief Executive) concludes that a personal data breach requires notification to the individual data subjects, they will ensure that the timing of such notification meets the ICO's requirements and the communication includes the following:
 - the name and contact details of [our Data Protection Officer];
 - a summary of the incident causing the breach;
 - the estimated date of the incident;
 - the nature and content of the personal data concerned (and whether it included any of the special categories of personal or financial information);
 - the likely consequences of the breach on the individual concerned (and, whether there is a risk of identity theft or fraud, physical harm or damage to reputation);
 - the measures taken by us to address the breach;
 - the measures that the individual could take to mitigate the adverse consequences of the breach and what we can do to assist them; and
 - a telephone number and/or email address the individual can use to contact us.
 - The Director of Administration and Corporate Services (or in their absence the Chief Executive) will also ensure that the means of communication is prompt and secure, in clear and plain language and that it is a specific message concerning the breach. It should not be combined with a communication on another topic.
- vi) **Other notifications**
- The Director of Administration and Corporate Services (or in their absence the Chief Executive) will consider whether any notification is required to be made to any other relevant regulatory bodies and make such other notifications as may be necessary in accordance with any applicable rules.
 - Where a notification is made to either the ICO or individual data subjects, the Director of Administration and Corporate Services (or in their absence the Chief Executive) is responsible for providing ongoing assistance to the ICO and/or individual data subjects as may be necessary or desirable in the circumstances.

- The Director of Administration and Corporate Services (or in their absence the Chief Executive) will liaise with the Board of Trustees prior to taking any actions or steps which may have legal or reputational consequences for Cambridge House.

e) Step 5 - Evaluation and response

- i) Once a breach has been contained, any notifications made and the immediate risks dealt with, the Director of Administration and Corporate Services (or in their absence the Chief Executive) will:
 - investigate fully the causes of the personal data breach, to identify whether any changes to our policies and procedures are necessary to reduce the likelihood of such a breach reoccurring; and
 - evaluate the effectiveness of our response to the personal data breach, with a view to implementing such changes to our procedures and/or chain of responsibility as may be necessary to ensure that any future personal data breaches are properly handled.
- ii) The Director of Administration and Corporate Services (or in their absence the Chief Executive) will ensure that the findings are recorded in a report. In the case of personal data breaches, which require notification to the ICO and/or data subjects, the report will be presented to the Board of Trustees, which shall agree the actions to be taken.
- iii) In the case of other personal data breaches, the Director of Administration and Corporate Services (or in their absence the Chief Executive) will determine what actions need to be taken to remedy any issues and shall file a copy of the report in a dedicated corporate services file along with the related Data Breach Record Form.

6. Is legal advice needed?

- a) In some circumstances, it may be clear that notification needs to be made to the ICO or individual data subjects and what the content of that notification needs to include.
- b) At other times, this may not be so clear. Where there is such uncertainty, legal advice will be sought by the Director of Administration and Corporate Services (or in their absence the Chief Executive).

7. Reviewing this policy

- a) This policy will be reviewed annually by the Chief Executive.
- b) Any questions regarding this procedure should be addressed to Katie Evans, Director of Administration and Corporate Services and Designated Data Protection Officer.

8. Retention of documents

The record of any personal data breach together with all correspondence or other documentation relating to the breach will be kept for a period of seven years.

Appendix 2a: Personal Data Breach Record Form

Personal Data Breach Record Form	
PART 1 - To be completed by the member of staff who becomes/is made aware of a personal data breach	
Name	
Job Title	
Date and time breach occurred	
Where did the breach occur?	
[Data Protection Officer/other] notified? Y/N	
Date, time and method of notification	
<p>What type of personal data breach has occurred – tick as appropriate?</p> <ul style="list-style-type: none"> ▪ Personal data has been accidentally lost or deleted by an employee. ▪ Personal data has been corrupted. ▪ Someone has accessed personal data or passed it on without proper authorisation. ▪ A network intrusion by a third party (e.g. a hacking incident or another type of cyber security attack). ▪ Data or equipment on which personal data is stored has been lost or stolen. ▪ Inadequate security controls (such as weak passwords) resulted in an unauthorised person gaining access to an IT system which includes personal data. ▪ Human error resulted in information being sent to the incorrect recipient. ▪ Personal data has been destroyed by unforeseen circumstances such as fire or flood. ▪ ‘Blagging’ offence, where information is obtained by deceiving the organisation who holds it has occurred ▪ Other (please specify) 	
What type of personal data is involved?	
Is any confidential or special category data involved in the breach e.g. medical/health information, financial information or personnel data? If so, what?	
What is the approximate number of individuals whose personal data are involved in the breach?	
Details of any individuals or organisations involved in the breach	

<p>Details of individuals or organisations that are aware of the breach, including details of when and how they became aware.</p>	
<p>Part 2 - For completion by the Director of Administration and Corporate Services (or in their absence the Chief Executive)</p>	
<p>The potential effect of the breach (e.g. potential loss of customer personal data)</p>	
<p>The potential cause of the breach</p>	
<p>Confirmation of any remedial action taken (e.g. hard drive wiped remotely within 6 hours of laptop reported as lost)</p>	

Appendix 2b: Personal Data Breach Risk Assessment Checklist

Personal Data Breach Risk Assessment Checklist	
1. What type of data is involved?	
2. Did the data include special category data (formerly sensitive personal data) e.g. health information?	
3. Did the data include data that was confidential, or which could be used to commit fraud or identity theft (e.g. bank details)?	
4. What could the data tell a third party about the individual?	
5. When did the personal data breach occur?	
6. What was the time lag between the personal data breach occurring and the discovery of the personal data breach?	
7. If data has been lost or stolen, are there any protections in place such as encryption?	
8. If data has been stolen, could it be used for purposes which are harmful to the individuals to whom the data relates?	
9. The measures taken or proposed to be taken to address the personal data breach, including any measures to mitigate its possible adverse effects.	
10. Assessment of whether the personal data breach should be notified to the ICO.	
11. Assessment of whether the personal data breach should be notified to individual data subjects.	

Appendix 2c: Guidance relating to notification of personal data breaches

1. Notification to the ICO

- a) Any personal data breach which is likely to result in physical, material or non-material damage to natural persons, such as:
 - i) loss of control over their personal data;
 - ii) limitation of their rights;
 - iii) discrimination;
 - iv) identity theft or fraud;
 - v) financial loss;
 - vi) unauthorised reversal of anonymisation;
 - vii) damage to reputation;
 - viii) loss of confidentiality of personal data protected by professional secrecy; or
 - ix) any other significant economic or social disadvantage to the natural person concerned.
- b) ICO guidance on the GDPR states that, to assess whether it is necessary to notify the ICO of a personal data breach, organisations should consider whether the breach is likely to have a significant detrimental effect on individual, such as:
 - i) discrimination;
 - ii) damage to reputation;
 - iii) financial loss;
 - iv) loss of confidentiality; or
 - v) any other significant economic or social disadvantage.
- c) If any personal data breach is likely to result in any of the consequences listed above, notification to the ICO should be made.
- d) If the personal data concerned was encrypted, a decision will need to be made as to the likelihood of decryption. If we can be confident that the personal data concerned remains secure, notification to the ICO may not be required. However, any such decision needs to consider the potential risks if the personal data were to become accessible to third parties.

2. Notification to individual data subjects

- a) Individuals must be notified when a breach of their personal data is likely to result in a high risk to their rights and freedoms.
- b) A “high risk” means that the threshold for notifying individuals is higher than for notifying the ICO and for example, may include personal data that:
 - i) Reveals the identify of vulnerable persons, including children;
 - ii) falls into the special categories of personal data set out in Article 9 of the GDPR;
 - iii) gives rise to a risk to individuals of financial loss, fraud or identity theft;
 - iv) has a high likelihood of causing damage to reputation or discrimination;
 - v) if it enters the public domain, the individuals concerned would suffer significant distress.
- c) Certain exceptions apply to the mandatory obligation to notify personal data breaches to individual data subjects. These are:

- i) Where appropriate technical and organisational protection measures have been implemented, and those measures were applied to the personal data affected by the personal data breach those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;
- ii) Where subsequent measures have been taken to ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialise;
- iii) Where notification would require disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

Appendix 3: Managing Vulnerable Clients' Data

1. Withholding information from a client	24
2. Working with people that may lack capacity	24
3. Recording Confidentiality Breaches Reasoning	25
4. Addition to Safeguarding	25

1. Withholding information from a client

There is a general duty to disclose details of all communications to the client regarding them. However, there may be exceptional circumstances in which this would not be in the client's best interests – such a situation must be justifiable as being in the best interests of the client (in all such circumstances this must be discussed with a line manager at the time or, if this is not possible, as soon as reasonably practicable after an initial decision is taken). Therefore, such an action must be given great consideration and an accompanying entry on AdvicePro or in the client records.

The rationale around this must demonstrate that either:

- a) providing such information would have, or has a realistic potential of being detrimental to the physical or emotional wellbeing of the person concerned; or
- b) providing such information would have, or has a realistic potential of being detrimental to the physical wellbeing of a third party; or
- c) providing such information would or has a realistic potential of interfering with the fair and proper investigation or adjudication of an allegation or complaint.

The intention of this is to prevent serious harm, or unjustified interference in proper investigation or adjudication. It does not provide a rationale for denying clients access to information except in highly exceptional circumstances. Staff and volunteers working directly with Cambridge House clients should make every effort to ensure that third parties do not disclose information to them that they do not wish to be disclosed to the client.

2. Working with people that may lack capacity

When working with clients, it may become apparent that a client does not have sufficient ability to provide us with the requisite consent to disclose or obtain confidential information about themselves. Explicit consent from an individual is required under GDPR and where this is not possible, the Mental Capacity Act 2005 applies.

In those circumstances Cambridge House staff/volunteers must take what steps they consider necessary in the best interests of that person. In forming a decision as to whether the person lacks capacity and what is in their best interests, a line manager (as appropriate) must be consulted. In making a best interests decision, the following factors should be taken into account:

- a) the ascertainable past and present wishes and feelings of the person concerned, and the factors the person would consider if able to do so;
- b) the need to allow for and encourage the person to participate, or to improve his or her ability to participate, as fully as possible in anything done for, and any decision affecting, him or her;
- c) the views of other people whom it is appropriate and practicable to consult about the persons wishes and feelings and what would be in his or her best interests; and
- d) whether the purpose for which any action or decision is required can be as effectively achieved in a manner less restrictive of the persons freedom of action.

Staff and volunteers need to be alert to differences of opinion between those who are consulted; the possibility of conflicts of interest between the client and their relatives, carers and close friends; and any relevant religious and cultural factors.

3. Recording Confidentiality Breaches Reasoning

An accurate written record must be kept of any decision to breach confidentiality. It contains all information relating to the decision. Where there has been consideration of a need to breach confidentiality, details of all information considered, the decision, persons consulted, and actions taken should be recorded.

4. Addition to Safeguarding

If you are working in a hospital and you are concerned about the risk of harm, following discussion with your line manager;

- a) Ensure that you have access to or an understanding of the hospital safeguarding policy as general best practice.
- b) Raise a concern as per the policy and check that the local authority have been informed.
- c) Retain your independence and if the hospital will not raise an enquiry or you are concerned that the issues are not being addressed in line with section 42 of the Care Act, contact the local authority and raise it with them.
- d) Ensure that if Advocacy is required due to substantial difficulty or a capacity issue, this is identified at the earliest juncture.