Data Protection Policy

Document owner:	Jan Winnington – Data Protection Officer
Current version:	1.4
Original created on:	2nd July 2018
Last updated on:	17th July 2018
Last updated by:	Stephen Bonfield – Compliance Manager

1. Introduction

1.1 Who this policy applies to

This policy applies in full to all staff, agents and volunteers of Christians Against Poverty ("CAP") in all departments and areas of the charity. Certain roles within CAP have particular areas of responsibility, as summarised in the following table:

Role	Area of responsibility in relation to data protection
Trustees	Have overall legal responsibility for ensuring that the charity complies with its legal requirements, including data protection. They will provide governance through board and committee meetings with senior management.
Senior Management Team	Also known as the "Core Team" – are responsible for the day-to-day running of the charity. They play a key role in promoting a strong culture of data protection throughout the charity, and ensuring that the necessary resources are in place to support this.
Company Secretary / Compliance Manager	Supports the trustees in understanding their legal duties, as well as providing support to the Data Protection Officer in technical, legal and contractual matters.
Head of Policy and Compliance	Leads the Policy and Compliance Team and provides oversight of and support to the Data Protection Officer.
Data Protection Officer	Is responsible for ensuring that policies and procedures are effective and comply with all relevant data protection laws. Acts as the point of contact for the Information Commissioner's Office ("ICO") as needed.
Director of Technology	Ensures appropriate technical safeguards are in place to secure the personal data of data subjects.
Department heads	Ensure appropriate organisational safeguards are in operation and are effective to secure the personal data of data subjects.
Team managers / leaders	Responsible for applying and enforcing this policy within own teams, and ensuring direct reports are adequately trained and supervised in their roles.
GDPR champions	Support the Data Protection Officer as a key contact within departments / teams in relation to data protection. Assists in the handling of data subject requests and team-based training.
Staff, agents and volunteers	Responsible for ensuring they are familiar with this policy and process any personal data in accordance with it.

1.2 Legal framework

The protection of personal data is regulated in the UK through various items of legislation, the most significant of which is the General Data Protection Regulation (EU) 2016/679 ("GDPR"), which entered into force on 25th May 2018. This is the main body of law agreed by the EU and which applies to all member states, including the UK.

The GDPR provides for member states to make further provisions that clarify certain areas that are left to their discretion, such as when to apply exceptions to the GDPR's obligations. In the UK, this is achieved through the Data Protection Act 2018 ("DPA 2018"), which received royal assent on 23rd May 2018. The DPA 2018 also incorporates the Data Protection Law Enforcement Directive 2016/680 into UK law, which deals with the processing of personal data for criminal law enforcement purposes.

Other relevant legislation includes the Privacy and Electronic Communications (EC Directive) Regulations 2003 ("PECR") – which regulates how personal data can be processed for direct marketing activities.

1.3 Data protection principles and role of the ICO

The GDPR sets out several principles that are fundamental to how personal data must be legally processed. This policy will set out how we comply with these principles and embed them into our procedures. The data protection principles relate to:

- Accountability – see section 2 below;
- Lawful processing of data – see section 3 below;
- Adequate, relevant and limited – see section 4 below;
- Accurate and up-to-date – see section 4 below;
- Retention and anonymisation – see section 5 below; and
- Security of data – see sections 6 and 7 below.

The ICO is the UK's data protection authority, established by statute to uphold information rights. The GDPR provides for the ICO to be able to use enforcement powers as part of its work, which can include fines of up to €20 million for the most serious breaches.

1.4 Terminology and external guidance

This policy uses terminology that has the same meaning as defined in the GDPR. For more detailed definitions, see GDPR Article 4 and the ICO's list of key definitions. In summary:

A "controller" determines the purposes and means of processing personal data.

A "processor" is responsible for processing personal data on behalf of a controller. An organisation can both control and process the personal data it holds. It can also use other organisations to process personal data on its behalf.

"Personal data" is any information relating to an identifiable person who can be directly or indirectly identified from it. Completely anonymised data can no longer identify a person and therefore falls outside of the scope of the GDPR.

"Pseudonymised data" is data that has been only partially anonymised – for example, by using a key-code (such as a CAP reference). Whether such data remains within the scope of GDPR depends on how difficult it is to attribute the pseudonym to a particular individual.

2. Accountability and governance

"The controller shall be responsible for, and be able to demonstrate compliance with, the other data protection principles." – Article 5(2) of the GDPR

The GDPR introduces an obligation on controllers to not only follow the data protection principles, but to be able to demonstrate their compliance with them. This policy is one of the means by which we are able to demonstrate fulfilment of this obligation and hence compliance with GDPR. This section will summarise the others ways in which we do this.

2.1 Processor contracts

Whenever we use third parties to process personal data on our behalf, we must ensure that there is a contract in place that complies with the requirements of the GDPR to transfer and further process that data. This can be done in two ways:

1. The required terms might be included in the main contract between CAP and the third party. The Company Secretary or Data Protection Officer must be sent a copy of the contract prior to us signing it in order to check and verify that the contract meets the required standards of GDPR;

2. Alternatively, if an existing contract does not contain the required terms, we must require the processor to sign an additional Data Processor Agreement. A template agreement for this purpose – **PC004 – Data Processing Agreement** – should be used. The Company Secretary or Data Protection Officer must be sent a copy of the completed template prior to us signing it in order to check that it has been completed correctly.

Further information around the terms that are required to be included can be found in our **Data Processor Agreement Policy**.

Whilst it is not a requirement of GDPR to have written agreements in place when sharing data with other controllers, it is best practice to do so particularly if the data sharing is on a large scale or regular basis. A template agreement for this purpose – **PC003 – Data Sharing Agreement** – can be used.

2.2 Documentation

Article 30 of the GDPR requires us to document particular aspects of our processing activities. This must be done in writing and must be at a sufficiently granular level of detail. The required information is contained in our **Data Mapping Schedule** held by the DPO.

2.3 Data protection by design and default

Data protection and privacy issues must be considered at the outset of every activity that CAP undertakes. This will be achieved by taking the following measures:

- We will consider data protection issues as part of the design and implementation of systems, services and practices;
- We make data protection an essential component of the core functionality of our processing systems and services;
- We anticipate risks and privacy-invasive events before they occur, and take steps to prevent harm to individuals;
- We only process the personal data that we need for our purposes and we only use the data for those purposes;
- We ensure that personal data is automatically protected in our IT systems, services and practices;
- We provide the identity and contact information of those responsible for data protection both within the charity and to individuals;
- We adopt a 'plain language' policy for any public documents so that individuals easily understand what we are doing with their personal data;
- We respect the preferences of our clients – for example, in respect of preferred contact methods;
- We only use data processors that provide sufficient guarantees of their technical and organisational measures for data protection by design.

2.4 Data protection impact assessments

A Data Protection Impact Assessment ("DPIA") is a particular form of risk analysis that examines the likelihood, impact and mitigation that can be put in place when processing personal data. It is a requirement under the GDPR to perform a DPIA before commencing any processing which "is likely to result in a high risk" to the data subjects. In particular, the GDPR says we must do a DPIA if we plan to:

- use systematic and extensive profiling with significant effects;
- process special category or criminal offence data on a large scale; or
- systematically monitor publicly accessible places on a large scale.

The ICO also requires us to do a DPIA if we plan to:

- use new technologies;
- use profiling or special category data to decide on access to services;
- profile individuals on a large scale;
- process biometric data;
- process genetic data;
- match data or combine datasets from different sources;
- collect personal data from a source other than the individual without providing them with a privacy notice ('invisible processing');
- track individuals' location or behaviour;
- profile children or target marketing or online services at them; or
- process data that might endanger the individual's physical health or safety in the event of a security breach.

Even if there is no specific indication of likely high risk, it is good practice to do a DPIA for any major new project, which may cover changes to an existing system, service or practice, involving the use of personal data. In order to ensure that the correct factors have been considered, the ICO's template DPIA should be used. Once completed, a copy of the assessment should be filed with the Data Protection Officer as CAP's central record.

2.5 Data Protection Officer

CAP has appointed a Data Protection Officer ("DPO") both as a matter of best practice and due to our core activities requiring large scale processing of sensitive personal data (such as financial details of our debt help clients) as well as some special category personal data (such as health information of our clients). The DPO's responsibilities will include:

- Informing and advising the charity of our data protection obligations;
- Monitoring compliance with the GDPR, including the assignment of responsibilities;
- Raising awareness of data protection and training staff;
- Providing advice to staff regarding the data protection impact assessments (DPIAs) and monitoring compliance and performance;
- Engaging with the Information Commissioner's Office as required.

2.6 Codes of conduct and certification

The GDPR recommends that controllers use approved codes of conduct and certification schemes on a voluntary basis to demonstrate compliance with best practice. At present, CAP is not a member of an ICO approved code of conduct or certification scheme. This will be

kept under review, and options for adhering to voluntary schemes will be considered as areas of future development.

3. Lawful processing of data

3.1 Lawfully, fairly and transparent

CAP will only process personal data once it has identified a lawful basis for doing so. This lawful basis will then be recorded in our **Data Mapping Schedule**. Article 6 of the GDPR sets out the following six lawful bases for processing data:

Basis	Summary
Consent	Any freely given, specific, informed and unambiguous indication of the data subject's wishes by clear affirmative action, signifying agreement to the processing. This will be a common basis that CAP relies on for processing personal data. See our **Consent Based Processing Policy** for more details.
Contract	Where the processing is necessary to fulfil our contractual obligations. We will mainly rely on this basis in relation to some aspect of HR processing of staff records.
Legal obligation	Where the processing is necessary to comply with a common law or statutory obligation. This is most likely to be relied on at CAP in the context of processing staff information.
Vital interests	Where the processing is necessary to protect someone's life. It is extremely unlikely that CAP would rely on this basis for processing.
Public task	Where the processing is done in the exercise of official authority (not relevant to CAP) or to perform a specific task in the public interest that is set out in law. It is unlikely that we would rely on this basis, and if we do, we must be able to specify the precise common law or statutory ground for doing so.
Legitimate interests	Where processing is necessary for our legitimate interests (or those of a third party), except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject. This will be a common basis for CAP to rely on. Before processing data on this basis, a **PC007 – Legitimate Interests Assessment** form must be completed and sent to Policy and Compliance. Details of the legitimate interest processing must also be brought to the attention of the data subject in a privacy notice.

The GDPR considers the following types of data to be a "special category", where in addition to one of the lawful bases above, and additional condition under Article 9 must be satisfied:

- race;
- ethnic origin;
- politics;
- religion;
- trade union membership;
- genetics;
- biometrics (where used for ID purposes);
- health;
- sex life; or
- sexual orientation.

When processing any of the above categories of data, our **Data Mapping Schedule** will set out the additional Article 9 condition being relied on. Personal data relating to criminal convictions is dealt with separately in Article 10 of GDPR. In practice, this means that CAP must – in addition to relying on one of the Article 6 bases listed above – also satisfy a condition provided for in the DPA 2018.

3.2 Specified, explicit and legitimate purpose

Our processing of personal data must be in line with the reasonable expectations of the individuals concerned. Our main privacy policy is available on our website at **capuk.org/privacy** and covers the main information which we are required to notify data subjects about. In addition to this, further privacy notices will be given at suitable stages where it is most helpful in ensuring the data subject is aware of how we will process their data. For example, debt help clients receive a further privacy notice in the **Things You Need To Know** booklet, and potential supporters will be informed whenever they complete a form to make an enquiry, donation etc.

4. Adequate, relevant and limited

We will process only that personal data which is necessary for the purpose we are using it for and no more. This means that we will design systems and processes that do not ask for or obtain unnecessary data.

4.1 Accurate and up-to-date

We will take proportionate steps to validate the data we hold to ensure its accuracy. For example, we obtain personal data from our debt help clients using an electronic fact find which incorporates data validation to ensure data entry is accurate. We will also ensure that personal data is up-to-date. For our debt help clients, this will include an annual review of their financial details and personal contact details. In relation to other individuals whose personal data we hold, we will provide a clear description in our online privacy notice explaining how we will respond to data subject requests for data to be rectified.

5. Retention and anonymisation

We will only retain personal data for as long as it is needed for the purpose we obtained it. In practice, there are a variety of retention periods depending on the nature of the data, which we set out in detail in our **Data Retention Policy** and **Data Retention Schedule**.

At the end of the retention period, we will either delete or anonymise the data. Anonymisation requires data to be rendered anonymous in such a way that the data subject is no longer identifiable. The Data Retention Schedule shows which of our IT systems will automatically anonymise data after the set retention periods.

6. Data security – technical measures

6.1 Security of physical files

Where possible, information is processed electronically on secure servers. Where this is not possible, paper records containing personal data must be stored either in locked filing cabinets or locked drawers. This applies equally to documents stored at head office, or in local centres. At the end of each working day or during extended periods of absence from your desk, desks must be cleared of all documents containing personal data and the documents must be stored securely in locked filing cabinets or locked drawers.

Our Bradford offices are physically secured by use of a keycard access system and monitored CCTV. They are also protected by a security alarm system and checked by a security firm after business hours.

Files that are archived pending destruction are stored in an archive room requiring either keycard or keypad entry. CAP's printers require staff keycards to be used to release the document, to reduce the possibility of printouts being left unattended.

6.2 Security of electronically stored information

There are a number of technical measures taken to ensure the security of data we hold electronically. These include:

- Systems are secured using password authentication, with password refreshes required at regular intervals.
- Mac laptops have their hard drives encrypted and are password protected;
- Firewalls are in place for all on-premises servers;
- Our external server provider includes firewalls as part of their service;
- Up-to-date anti-virus software is installed on all machines;
- Old hard disk drives are wiped with multiple passes before being destroyed by a specialist firm;

- External IT contractors are tendered and referenced before being contracted and sign a non-disclosure agreement.

In addition to the above, we operate intrusion-detection and security monitoring software and employ system penetration testing at regular intervals. Remotely based staff, including centre staff, must ensure that their use of IT equipment satisfies the requirements set out in the IT department's **Information Security Policy**.

Files containing personal data that are to be shared with external third parties must be transferred using a secure method. If a CAP system, such as the creditor portal, cannot be used to transfer the information, the file should be encrypted following our **Guide to using Firefox Send**.

7. Data security – organisational measures

7.1 Training

All new starters at CAP attend training on the use of IT systems, including the importance of keeping passwords confidential and secure at all times. Staff and agents receive annual refresher training which includes a summary of the key points in relation to the GDPR and information security training. This is followed by a requirement to declare that the training has been undertaken and understood, and a short test to monitor the effectiveness of the training. Staff and agents also undertake role-specific training, aimed to address the issues most relevant to their day-to-day work.

7.2 Confidentiality and offences under the DPA 2018

We are committed to providing confidential services to our clients and the GDPR requires us to only share information with others when we have a lawful basis for doing so. Confidential information in this context includes, but is not limited to, any personal data as defined by Article 4 of the GDPR. All staff, volunteers and agents are bound by specific duties of confidentiality, which can be found in our staff contracts, volunteer confidentiality agreements and agency agreements respectively. We will also require any third party contractors who have access to personal data we hold to include confidentiality clauses in their agreements with us.

Centre Managers and Debt Coaches are responsible for ensuring that Support Team Volunteers and Befrienders have signed the **Support Team Agreement** (which covers issues such as conduct on visits, personal safety and confidentiality) before doing any visits and getting access to any client data. This can be found on the Intranet in the Debt Centres Support Team folder.

Centre Administrators need to sign a more detailed **Confidentiality Agreement** (which also covers Data Protection) due to their access to CAP computer systems. This is also available on the Intranet.

A copy of the signed agreements should be kept in a filing cabinet in the office – Area Managers will check this data annually and Regional Leaders will check on the accompanied 3-month visit to ensure compliance.

Any visitors to head office who are likely to be exposed to confidential information – for example, because of being given a tour of our offices – will be required to sign **PC002 – Non Disclosure Agreement Visitors**, unless they are already bound by confidentiality due to a separate contract with us or their own legal duties. We will also require any observers attending debt help visits with clients in their homes to sign **PC006 – Non Disclosure Agreement Debt Help**, again unless they are already bound by confidentiality – for example, under a befriender confidentiality agreement.

Staff, volunteers and agents **must not** access, or attempt to access, personal data relating to our data subjects – for example: clients, supporters and other staff members – **unless** it is a necessary part of their role. It may be a criminal offence under the DPA 2018 for an individual to:

- Obtain personal data CAP holds, without CAP's permission (s.170);
- Re-identify personal data CAP holds, without CAP's permission (s.171);
- Alter, deface, block, erase, destroy or conceal information that a data subject has requested access to, after they have made the request (s.173).

7.3 Client confidentiality

A client's identity and details must not be passed to any other members of staff, volunteers or agents except in situations where it is a necessary part of performing their role as authorised by CAP. All clients should be able to access our service in confidence, without a risk that others – including members of the local church network – being told without their consent. Meetings with clients outside of a client's home should be held in a confidential space. Centre staff should not confirm the client's presence in the centre or use of the centre without first obtaining the client's consent.

7.4 Overriding confidentiality – including safeguarding and police requests

There may be exceptional occasions where CAP workers feel they need to breach confidentiality. This should be treated with the utmost care, as any breach of confidentiality may not only harm the rights of the individuals in question, but also damage our reputation and lead to legal action against us. The following steps must therefore be taken:

Step	Action by individual considering whether to override confidentiality
1	Consider whether the matter relates to a safeguarding concern. If so, follow CAP's separate **Safeguarding Policy** and not the remainder of this procedure.
2	Consider whether the matter relates to a request for information from the police /

	investigators. If so, follow CAP's separate **Criminal Investigations Disclosures Policy** and not the remainder of this procedure.
3	If the above do not apply: immediately raise the matter with your line manager. Explain why you feel confidentiality should be overridden and what would be achieved by breaching confidentiality. The line manager must take a written note of this discussion.
4	Subject to step 5 below, the line manager is responsible for discussing the available options with you, and making a decision on whether to make the disclosure. A record should be made identifying the lawful basis under the GDPR / DPA 2018 that permits the disclosure of the personal data in the circumstances. The Company Secretary or Data Protection Officer should be consulted if necessary.
5	If the data subject is a debt help client, the line manager should pass the information on to the relevant Debt Ops Team Manager, who will take the action set out in step 4 above in place of the line manager.
6	The decision of the line manager (step 4) or Debt Ops Team Manager (step 5) is the final decision of Christians Against Poverty. In no circumstances should the matter be discussed at this stage with any other member of the senior management team or board. This is to ensure that any future complaints or investigations arising from a breach of confidentiality can be carried out in an independent manner.

7.5 Information security policy and cyber security risk log

The Information Technology team will maintain an **Information Security Policy**, which all members of staff, volunteers and agents must make themselves familiar with. They will also maintain an **internal Cyber Security Risk Log**, and review this every quarter.

7.6 Data breach protocol

We will ensure that we are well prepared in planning our response to dealing with a potential data security breach. In the event of a data security breach, staff must follow the Data Breach Protocol, which can be found in *Appendix B*, below.

7.7 Statistical monitoring

Where data is processed for statistical analysis or research purposes, it should be processed in an anonymised form unless it is absolutely necessary to include personal identifiers. Large-scale statistical analysis using personal data (i.e. data that has not been effectively anonymised beforehand) is likely to require a Data Protection Impact Assessment to be completed to address the potential risks involved (see 2.4 above).

7.8 Transfer of data

The GDPR imposes restrictions on the transfer of personal data outside the European Union, to third countries or international organisations. These restrictions are in place to ensure that the level of protection of individuals afforded by the GDPR is not undermined. Personal data may only be transferred outside of the EU in compliance with the conditions for transfer set out in Chapter V of the GDPR.

CAP's main servers are hosted in the UK, and we would not ordinarily process any personal data with organisations outside the UK. We do however use G-Suite servers operated by Google LLC for collaborative work and as our company e-mail server, which may contain incidental personal data relating to data subjects. We have chosen G-Suite as our provider of these services due to their high security standards, which conform to the standards of the EU-US Privacy Shield. We have therefore noted the potential for transfer of personal data outside the EU in our online privacy notice.

7.9 Explicit consent

Explicit consent is the normal mechanism for ensuring that special category data (see 3.1 above) can be processed under GDPR. In respect of our debt help service, this is most likely to be encountered when processing a client's health information to share with their creditors. A **Health Permission Form**, available on HOPE, should be signed by the client, scanned and recorded on the 'Access and Health' page on HOPE where consent has been granted. The Access and Health page should be where current information about the client's health is stored, and this should be kept updated.

Health information may also be recorded historically in other places – such as casenotes, visitnotes and printed letters. The reason for this is that our casework is audited both internally (by the QA Officer) and, from time to time, externally (by our regulator the FCA, or standards bodies such as MAS). In order to demonstrate that we have given the correct advice, it is sometimes necessary to be able to see what the client's health situation was at that time.

If we simply deleted all references to old health conditions in the casenotes, it might afterwards appear negligent that we have given the client certain advice (for example, about incapacity benefits). It would also be difficult for auditors to spot when we haven't given appropriate advice (e.g. if we delete mention of a health condition, the auditor won't spot it we have failed to give correct advice about it).

A client has the right to withdraw consent at any point. This will most often be consent **to share** information:

- The caseworker should update the consent level in the Access and Health tab.
- The caseworker should contact creditors to ask them to remove info from their systems
- The caseworker should arrange for any Explicit Consent form scanned on to be deleted.

If a client wants us to delete all mention we have of a health condition (e.g. **to store** the information internally), you should explain that we normally need to keep a historical record of information we had for audit purposes (see above), but that we will delete the "live" information in the Access and Health tab. If the client does not agree with us retaining the information for this purpose, please consult the Data Protection Officer for advice.

The Data Protection Officer will then consider if there are exemptions under Article 9(2)(f) of the GDPR or the DPA 2018 Schedule 1 allowing us to continue to process this special category data without consent, and if not, how best we can remove references of the health information without undermining the ability of our advice to be properly audited.

7.10 Data Audits

There will be regular internal assessments across each department to ensure we all understand and are meeting our data protection obligations. These data audits will be undertaken on a regular basis requiring participation from every team at Head Office and a selection of our centres for each frontline service. The audits will be planned, scheduled and performed by the DPO and recommendations on how to improve will be made to each department Head.

8. Individual rights

The GDPR grants an individual rights over their data. The availability of these rights depends on the lawful basis that the data was processed on, and whether any exceptions under either the GDPR or the DPA 2018 apply. The GDPR provides the following timescales for complying with data subject requests:

Data Subject Request	Timescale
The right to be informed	At the time the data is collected (if supplied by data subject) or within one month (if not supplied by data subject)
The right of access	One month
The right to rectification	One month
The right to erasure	Without undue delay
The right to restrict processing	Without undue delay
The right to data portability	One month

All staff, volunteers and agents must be familiar with and follow the **Data Subject Request Procedure**.

Appendix A – Security related procedures

1. Caller verification

Before discussing a data subject's personal details by telephone with an individual purporting to be the either the data subject themselves or an individual who the data subject has given their consent for us to speak with (for example, third party with authority, their creditors, etc.), all members of staff must verify the caller's identity.

Note: it may not always be necessary to verify a caller's identity if they are not requesting personal data – for example, a client's family member who is calling to give us information about the client's situation. However, we would remain bound by confidentiality – including the requirement to not confirm, without the client's consent, that they are indeed working with us.

The following table sets out the questions that should be asked to verify identity:

Category of caller	Procedure for identity check
Client	A debt help client must answer 3 of the following questions correctly for us to be sure that we have verified the client's identity. Please ask these questions in order: • CAP reference number • First line of their address and postcode • Their date of birth • Are you renting or a house owner • Their middle name (or partner middle name) – if they have one recorded on details • Their child's name – if they have one recorded on the details screen • National Insurance number • Email address – if recorded on the details screen • A previous address – if they have one on the details screen A client of another CAP service must answer 3 of the above questions where applicable (i.e. where we hold this information to check against).
Creditor of debt help client	A creditor must answer 3 of the following questions correctly for us to be sure that we have verified their identity. Please ask these questions in order: • CAP reference number

- Client's name
- The client's first line of address and postcode
- The creditor's reference number

Third party authorised by debt help client

A third party must already be authorised by the client in order for us to discuss their account. Once it has been confirmed that the third party has authority, the identity of the caller then needs to be checked by correctly answering 3 of the questions in the following order (or alternatively by providing a password if one has been set up):

- CAP reference number
- First line of client's address and postcode
- Client's date of birth
- Is client renting or a house owner
- Client's middle name (or partner middle name) – if they have one recorded on details
- Client's child's name – if they have one recorded on the details screen
- Client's National Insurance number
- Client's Email address – if recorded on the details screen
- Client's previous address – if they have one on the details screen

Debt coach

When contacting Debt Ops, all debt coaches will need to provide a passcode in order to prove their identity. The passcode is available on the Debt Centres section of the intranet documents system under 'Passcode'. It is updated weekly. If the debt coach is unable to provide this code, they will need to answer two security questions about their centre (including: phone number, address, line manager, days worked).

Please note that only the Debt Coach or a person with third party authority for that client can contact Debt Ops about a case. Support team members cannot contact Debt Ops to give or receive information about a client case.

Supporter

An existing supporter must answer 2 of the following questions correctly for us to discuss their personal information or make amendments to their contact details:

- First line of address and postcode
- As above, for previous address(es)
- Supporter's date of birth (if known)
- Supporter's e-mail address – if known
- Supporter's telephone number – if known

Other	In all other cases – individuals should be asked 3 security questions relating to information which we have on our relevant systems which it would be reasonable for us to expect the genuine data subject to know. Where a procedure has been put in place to set up a password to confirm the identity of the caller, this may be used in place of the security questions.
ID checks have failed	If a caller is unable to answer a security question, they should be asked an alternative from the list (where possible) up to 6 questions in total. If the caller has still not given the correct responses from these questions, the caller should be informed that they have failed security and would need to write to us with proof of identity to allow us to process their request. A casenote should be made recording the time of the call and the fact that security was failed. If multiple attempts to access information are made by a caller who fails security, the Data Protection Officer must be informed. Remember that we can still take information from callers without confirming ID, but are unable to share personal data on our records or confirm that the individual they are claiming to be is a client / supporter.
Exception – Discovery Break calls	We may receive a request from a debt coach to invite a client to one of several client breaks that we run during the year. The team that calls the client to book these breaks is deliberately only given a small amount of detail relating to the client, so that they only have what is necessary to book the break (i.e. not the client's entire case management record). This team will therefore not be able or be required to ask a series of security questions. However: (1) the team should still refuse the call if for any reason they become suspicious; (2) the team do not have access or authority to change the client's case records, or take any action in relation to the client over and above what is necessary to book the client on to a break.

2. Working From Home

In some circumstances, managers can authorise staff to perform some work remotely from their home. This helps us to provide flexibility in our working environment where it is appropriate to do so. Where this work might involve processing personal data, particular care must be taken.

- WiFi must be suitably password-protected and of an adequate encryption type. Unsecured WiFi must not be used. If in any doubt, a wired connection must be used.
- The PC equipment must be adequately protected (antivirus, password, screen lock) and no one else in the home should be able to see any personal data (either on screen or in print) or overhear conversations.
- Work must be done in a closed room with no interference from other people.
- CAP has not done Health and Safety assessments of staff homes, however, if a member of staff decides to work from home they need to be safe. This includes using a desk or appropriate table.
- If the computer at home is shared, a 'CAP' user with appropriate password protection must be created so that systems such as HOPE cannot be accessed by other users of the computer.
- The worker must NEVER save files containing any personal data to their personal computer equipment, or take documents home on a USB stick. Personal data should only be accessed within CAP's web-based secure systems (HOPE, JOY, etc.)
- Any personal data that is incidentally downloaded to the computer (for example, as a result of opening an e-mail attachment on viewing a document as a PDF) must be immediately deleted from the downloads folder of the computer.
- The **Working From Home declaration** form must be signed by the worker before they are permitted to work from home.

Additional Debt Ops Requirements

For staff who work in the debt operations department and who have access to debt help client data, the following additional requirements must be met:

- In the event of unforeseen circumstances, the manager may at short notice (24 hours) cancel the working from home day;
- A caseworker must report to their Team Manager at the beginning of the day;
- The working from home day cannot be tagged on to a holiday (either the day before the holiday or the day after);
- Working from home is not available to interns in Debt Ops;
- There will be a maximum of 2 working from home days per month for each caseworker;
- A caseworker must have passed probation and be signed off to produce Financial Statements With Advice;
- Working from home days can only be requested up to 2 months in advance.

3. Transporting personal data out of head office

Whenever paperwork that contains personal data is removed from Head Office – for example, when working from home – consideration must be given to ensure that it remains

secure at all times. CAP will take a risk-based approach to the measures required in order to ensure this security.

Moving personal data paperwork between buildings

As both buildings on site (Jubilee Mill and Jubilee Centre) are very close together, the risk to any paperwork being moved between buildings is relatively low. However, the following issues must be considered:

- Paperwork should be taken directly to the other building without any delay;
- Paperwork should be covered to prevent any damage by weather;
- If transporting a large amount of paperwork, the risk of sheets being lost on route may be greater. Extra care should therefore be taken and it may be appropriate to secure the paperwork in a zipped bag.

Taking personal data paperwork home by car

As a car is a private and relatively secure method of transport, the risks to any paperwork being transported are less than if travelling by public transport or walking. However, the following issues must be considered:

- Paperwork should be taken directly from the building to the car without any delay;
- If the walk to the car from the building is more than a short distance (around 20 metres), or if transporting a large amount of paperwork, it may need to be secured in a zipped bag;
- Locking paperwork in the boot of the car before travelling will be more secure than leaving paperwork on a passenger seat;
- Care must be taken to ensure that all of the paperwork is removed from the car, and that sheets do not become loose and get lost or left behind;
- Extra care should be taken if travelling in someone else's car (i.e. when getting a lift home) to ensure that paperwork is not left in the car, and that client details cannot be read by other passengers.

Taking personal data home by public transport / walking / cycling

This form of transport has the most potential risk to the security of the paperwork being moved. Risks include accidental loss of paperwork and subsequent access to the public and the theft of bags containing paperwork. For these reasons, the following requirements must be met:

- Consideration must be given as to whether it is *absolutely necessary* to remove the paperwork from Head Office. If the same information can be accessed via a secure internet connection (e.g. through HOPE) this should be preferred;

- Any caseworker taking paperwork home must use a lockable pilotcase or briefcase *provided by CAP*. There is a store of cases both in Jubilee Mill (in Client Setup) and in Jubilee Centre (in Insolvency).
- Each case is colour-coded, and the caseworker must check the online log to ensure that a case is available to be used. The log can be accessed on the server at **Debt Ops : Public : Data Protection : Briefcase log**.
- The briefcase must be "signed out" of CAP by completing the online log, including who is taking the case and when it was taken.
- Once paperwork is inside the case, the case must be closed and the 6-digits of the combination lock must be rolled to ensure the case is locked. It is not acceptable to just close the case without making sure it is locked. When the case is opened again, the combination code must not be changed.
- Once the paperwork and case are back in Head Office, the case should be returned to its original storage place, and the log must be completed to record that the case has returned and is available for others to use.

4. Use of messaging services

In order to facilitate collaboration and efficient communication, CAP may utilise internal messaging services such as iChat, HipChat and others. These are work tools and not a replacement for private social media. Staff should not write anything they wouldn't ordinarily write in a work e-mail. These platforms are intended to be used for *general* conversations that a member of staff might otherwise have when phoning a colleague, emailing them or talking to them at their desk.

In particular, caseworkers should not use messaging services to discuss *specific* personal data. Debt help case information should only be conveyed through an Internal Communication. This is because (a) an Internal communication will make sure we have an accurate record of work / discussions on a case and (b) anything specifically relating to a client must be securely communicated.

5. Third party authorities

If a debt help client has a friend or family member, a support worker, or any other individual who the client wants us to deal with on their behalf, signed authority must first be obtained and scanned onto HOPE. Until this is done, the caseworker is not to disclose information about the case to that individual. This is to ensure maximum protection for the client. The only exception to this would be where we receive a 'one off' call from a third party, and have been granted verbal authority from the client on the call. In such an instance, the case worker must clearly case note that this took place and ensure that a third party authority is in in place for any subsequent calls.

Once the necessary authority has been received and scanned on, the caseworker should mark the details of the approved individual as a Key Issue for clarity to others accessing the

case. Where we hold a Third Party Authority on HOPE we can accept a request for a withdrawal of the clients savings from the Third Party. However, if the bank account details to which the savings are to be sent are different from those held on the clients' CAP Plan, then the client needs to call themselves to request the change to the details and to make the withdrawal.

6. Befrienders

Befrienders play a vital role in offering support to our clients, however they should not in any way be involved in the debt counselling process itself. Subsequently it is not part of their role to know any details surrounding the financial aspect of the client's case and they should not be calling into Head Office on the client's behalf. If a befriender does call into Head Office the caseworker should be mindful not to divulge any information regarding the client's case, unless authority from the client has been obtained. The only acceptable exception to the above statement would be where the client requires a significant, on-going level of support from the befriender. In the event of this we request that a signed Third Party authority is obtained and scanned onto HOPE. In the absence of a signed Third Party authority the caseworker is not permitted to disclose any information.

7. Checking outbound post

Any outbound post containing personal data must be carefully checked to ensure that the contents are intended for the addressee. This is particularly relevant for manual letters being sent from Debt Ops, especially in relation to ensuring any enclosures (such as Financial Statements, wage slips, original paperwork being returned, etc.) matches the person the letter is addressed to. The check should be for each sheet of paper / enclosure, and care must be taken to check that the name and address matches the client's records on HOPE.

Caseworkers must then use the green stamp near the post trays to stamp the reverse of the sealed envelope to confirm that the contents have been checked. Post created by caseworkers should not be leaving the building without first being carefully checked and then stamped to confirm the check has happened. Caseworkers must take care to avoid the following potential risks:

- Letters being printed and left on the printer. The next person to print a letter may then pick up the whole bundle and assume it all belongs to their client.
- Paperwork being placed on the wrong file to begin with (either physically in the wrong paper file, or electronically, by being scanned on to the wrong case).
- Where there are a lot of enclosures, it is easier to overlook one item and more care needs to be taken.
- Caseworkers should not assume that paperwork in the same name but at a different address belongs to their client. Check HOPE for a record of previous addresses to make sure.

8. Centre staff

Centre staff – including debt help agents and group service coaches – must follow the same data security technical measures as outlined above, where this is relevant to the context of working in the local centre. In addition:

- Centre staff must use a designated computer and ensure that the computer is secured or logged off when not in use.
- Centre staff are *not* permitted to electronically hold personal or confidential data relating to clients outside of CAP's secure systems.
- Centre staff's computer accounts should be password-protected and the password should be regularly changed, 'strong', and not be known to others.
- Information about a client's case should not be viewed within sight of, discussed with or near anyone who does not have a right to know the information, unless the client has consented to the information being shared.
- When transporting paperwork – e.g. between a client's home and an Agent's office – care should be taken to keep the paperwork secure and confidential.

It should not normally be necessary for debt help agents to keep copies of client paperwork, as this should be sent to head office by post as soon as possible after a visit.

Agents must be aware that retaining copies of client paperwork presents additional data protection risks, exposing clients to the risk of identity theft and fraud if the documents are stolen or misplaced, and exposing CAP to potential enforcement action, fines and reputational damage.

If for any *exceptional* reason copies of client paperwork are retained by the agent, they should only be kept until the relevant Debt Ops team has confirmed receipt of them and then must be securely destroyed. All case records must be locked away at the end of each working day in a dedicated lockable filing cabinet. **Under no circumstances should client paperwork be stored with valuable items, such as laptops, which are more likely to be targeted for theft.**

Appendix B – Data Breach Protocol

CAP processes large amounts of sensitive data – in particular, financial details of debt help clients and supporters and – in some cases – special category relating to our clients. We are committed to respecting and protecting the privacy of the information we hold and every care is taken to protect personal data and to avoid a data security breach. This policy outlines our actions and response in the event that a security breach occurs.

What constitutes a data breach?

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data. For example:

- access by an unauthorised third party;
- deliberate or accidental action (or inaction) by a controller or processor;
- sending personal data to an incorrect recipient;
- computing devices containing personal data being lost or stolen;
- alteration of personal data without permission; and
- loss of availability of personal data.

There are four important elements to our breach management plan:

A. Containment and recovery
B. Assessing the risks
C. Notification of the breach
D. Evaluation and response

A. Containment and recovery

Data security breaches require not just an initial response to investigate and contain the situation but also a recovery plan including damage limitation. This will involve specialists such as IT, HR and in some cases legal and/or external stakeholders and suppliers.

If the security breach involves any aspect of technology (for example, a password is compromised) the person who discovers the data security breach must immediately inform the IT Helpdesk.

The Data Protection Officer, together with any relevant department heads, will determine the appropriate course of action and required resources needed to limit the impact of the breach. This might require isolating a compromised section of the network, alerting relevant staff or shutting down critical equipment.

Appropriate steps should be taken to recover data losses and resume normal Charity operations. This might entail attempting to recover any lost equipment, using back up mechanisms to restore compromised or stolen data and changing compromised passwords.

In the case of machine breach, the affected computer should be turned off and/or unplugged from the Internet immediately.

B. Assessing the risks

Upon discovering a data security breach, the Data Protection Officer and Head of Policy and Compliance must be immediately informed. The Data Protection Officer and Head of Policy and Compliance should be given the following information:

- What data is involved;
- Who are the individuals affected;
- Full and accurate details of the incident, including who is reporting the incident, what type of data was involved and how many people are involved.

The Data Protection Officer – or if unavailable, a person appointed in their place – will be responsible for investigating the data breach.

The investigation should consider the extent of the sensitivity of the data, and assess the risk as to what the consequences may be for the data subjects involved and the potential impact on the charity.

Some data security breaches will not lead to risks beyond possible inconvenience to those who need data to do their job – for example a laptop is irreparably damaged but files are backed up and can be recovered. This is a much different risk to the theft of a client database whose data may be used to commit identity fraud. Before deciding on what steps are necessary, further to immediate containment, we need to assess the risks, which may be associated with the breach and the potential adverse consequences to the individual.

- Is the data sensitive or of a very personal nature for example financial or health information?
- Does it contain bank account information?
- Was the data encrypted?
- How many individuals' personal data is affected by the breach?

In addition to addressing the risks to data subject, it is also necessary to inform our PR Officer to ensure that reputational risks can be considered and prepared for, and that there is PR involvement in any notifications to data subjects (see below).

C. Notification of the breach

Under the GDPR, CAP has a duty to notify the ICO about certain types of data protection breaches. If there is a "high risk" of data subjects' rights and freedoms being adversely affected then those individuals must also be informed.

Breaches CAP needs to notify the ICO about

The GDPR states that the ICO should be notified of a personal data breach *"unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons" (GDPR Article 33).*

Failing to notify the ICO about a breach when required to do so can result in a significant fine up to €10 million euros. This means it is crucial to establish the likelihood that individual's rights and freedoms are at risk as a result of the breach, and the severity of this risk.

If it is unlikely there is any risk then the ICO does not need to be notified, but details of the breach should be documented as CAP is required to be able to justify the decision not to inform the ICO.

- For example, the loss of a memory stick that was appropriately encrypted may not need to be reported to the ICO.

A data processor is a third party that processes information on behalf of an organisation. If a data processor suffers a breach then they are required under GDPR to inform CAP without delay. It is then CAP's responsibility to notify the ICO in line with this policy.

The GDPR states that an organisation must report a relevant breach to the ICO no later than 72 hours after becoming aware of it. If notification takes longer than 72 hours, CAP must provide reasons for the delay. It may not always be possible to fully investigate a breach in the 72 hour time frame, so the GDPR also allows for information to be required in phases as long as his is done without undue delay. It is still important to notify the ICO immediately, to explain the delay and give an idea of when full details can be submitted.

What must a breach notification to the ICO contain?

When reporting a breach, the following information must be provided under the GDPR:

- a description of the nature of the personal data breach including, where possible:
  - the categories and approximate number of individuals concerned; and
  - the categories and approximate number of records concerned;
- the name and contact details of the data protection officer or other contact point where more information can be obtained;
- a description of the likely consequences of the personal data breach; and

- a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

In practice, CAP will use the notification forms provided by the ICO on their website.

Notifying data subjects affected

If a breach is likely to result in a "high risk" to the rights and freedoms of data subject, those concerned must be contacted directly and without undue delay. This is particularly important where there is an immediate risk of damage that needs mitigating. Individuals should be given guidance on how to protect themselves from the effect of the breach.
The above means it is crucial to establish the likelihood that individual's rights and freedoms are at risk as a result of the breach, and the severity of this risk. If it is decided that we do not need to notify individuals then the reasons for this decision should be recorded. The ICO does have the power to compel organisations to inform individuals if they deem it necessary, and CAP needs to be able to justify the decision not to do this.

Examples

- CAP suffers a breach that results in an accidental disclosure of client records. There is likely to be a significant impact on the affected individuals because of the sensitivity of the data and their confidential details becoming known to others. This is likely to result in a high risk to their rights and freedoms, so they would need to be informed about the breach.

- CAP experiences a breach when a member of staff accidentally deletes a record of supporter contact details. The details are later re-created from a backup. This is unlikely to result in a high risk to the rights and freedoms of those individuals. They don't need to be informed about the breach.

What information must we provide to individuals when telling them about a breach?

Individuals should be informed of the nature of the personal data breach, and given the following information:

- the name and contact details of CAP's Data Protection Officer
- a description of the likely consequences of the personal data breach
- a description of the measures taken, or proposed to be taken, to deal with the personal data breach including any measures taken to mitigate possible adverse effects.

The above are required by the GDPR, but it may also be appropriate to offer advice to the data subject regarding actions they may be able to take to reduce the risks associated with the personal data breach.

Other notifications

Depending on the seriousness and nature of the security breach, it may also be necessary to notify the Police, FCA (see Principle 11) and the Charities Commission.

D. Evaluation and response

It is important not only to investigate the causes of the breach but also to evaluate the effectiveness of our response to it. Clearly, if the breach was caused, even in part, by systemic and on-going problems, then simply containing the breach and continuing 'business as normal' is not acceptable. We should ensure that:

- We know what personal data is held and where and how it is stored.
- Establish where our biggest risks lie.
- Ensure that the method of the transmission of any personal data is secure.
- Identify weak points in our existing security measures – for example staff storing client data on home computers.
- Monitor staff awareness of security issues and look to fill any gaps through training or advice.
- Have an identified group of people responsible for reacting to reported breaches of security.

Once a serious breach is contained, a thorough review of events will be undertaken by the Core Team to establish the cause of the breach, the effectiveness of the response and identify areas that require improvement.

Recommended changes to systems, policies and procedures will be documented and implemented as soon as possible after the incident.