

## Data Protection, Confidentiality and Privacy Policy

<b>Document owner:</b>	Ros Thomas – Centre Manager
<b>Current version:</b>	1.0
<b>Original created on:</b>	9 <sup>th</sup> Oct 2018
<b>Last updated on:</b>	21 <sup>st</sup> Jul 2021

### Data protection policy statement and purpose

As Agents of Christians Against Poverty you will hold and have access to large amounts of sensitive data and personal information about our clients. CAP is fully committed to respecting and protecting the privacy of the information we hold and every care should be taken to protect personal data and avoid a data protection breach.

#### Introduction and legal context

Christians Against Poverty holds and processes personal details in accordance with the Data Protection Act 1998 and is registered with the Information Commissioner, as a data controller.

The Data Protection Act 1998 (DPA) makes provision for the regulation of the processing (use) of information relating to individuals, including the obtaining, holding, use or disclosure of such information. The Information Commissioners Office (ICO) investigates any data protection breaches and since April 2010 the Information Commissioner has been able to impose fines of up to £500,000 as a penalty for serious breaches of the DPA.

Principle 7 of the Data Protection Act 1998 states that organisations which process personal data must take 'appropriate technical and organisational measures against the unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.' In practise this means that we must have appropriate security to prevent the personal data we hold being accidentally or deliberately compromised and be ready to respond to any breach of security swiftly and effectively.

It is the responsibility of all our Agents to ensure that they comply with the Data Protection Act 1998. As a practical outworking of this, our Agents should ensure that they use a designated computer and that the computer is secured or logged off when not in use. Agents are not permitted to electronically hold personal or confidential data relating to clients outside of CAP's secured systems. Agent'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. Any paperwork relating to clients should be locked away. When transferring paperwork between a client's home and an Agent's office, every care should be taken to keep the paperwork secure and confidential – please refer to the Confidentiality Agreement for more information regarding your responsibilities.

In 2017 we decided to bring our centre staff into line with head office staff and provide annual data protection training followed by a brief assessment.

### Your personnel information and records

Personnel files are kept securely in locked drawers in the Debt Centre team and Quality Assurance Departments and on CAP's secure IT systems.

The information contained in these records includes personal data, sensitive personal data, details of jobs held and information on performance and conduct. The information is used to assist with appointment decisions and in managing an Agent's performance, as well as for authorising you as our

Agent. It is also used to provide management information.

We make every effort to ensure that information is held securely and we comply with legislative requirements in terms of allowing you access to the information held on you. Should you wish to view your information, you may do so at any time by sending a request to the Head of HR. We will aim to deliver a copy, in your preferred format, of any information requested within seven working days. If any of the information is inaccurate, please let us know and provide full details so that we may correct this.

We will not ask you for, or record on paper or electronically, personal information, which is not necessary for us to operate effectively. We will also do our best to keep your information safe, accurate and up-to-date.

We will not give out your personal details to any external body unless these are required for the purposes of health and safety reasons (e.g. medical condition), or a criminal or PAYE investigation (please see section 5.5, Releasing information to detect or prevent a crime) etc. We will only give references for employment references if you have given your permission for this.

### Our clients' personal information and security questions

During the course of your contract as our Agent if you have access to, or reason to handle, our clients' personal information, you must always comply with the Data Protection Act. If you are unsure of the current legal requirements, please check with the Director of HR.

When clients contact Debt Ops teams they will be asked 3 security questions on each phone call due to the level of information exchanged. For conversations between Agents and clients we would only expect security questions to be asked if a client requests detailed information about their case or if the Agent suspects that the caller is an imposter. Security questions should be taken from information in HOPE such as date of birth, middle name, previous names, address, previous address, frequency and amount of current payment to CAP.

### Contacting Debt Ops

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 you are unable to provide this code, e.g. you are out of the office and cannot remember it; you will need to answer two security questions about your 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.

### Sensitive personal data

The Data Protection Act 1998 creates additional safeguards in relation to the processing of "sensitive personal data", which includes a person's "physical or mental health or condition". In relation to our debt counselling, this information is usually used to explain a client's situation more fully to creditors, which can result in creditors being more understanding and supportive towards us and the client.

Our standard Client Authority is not sufficient for us to pass on information about a client's health to creditors. The fairest way of ensuring that we meet the requirements of the Data Protection Act is to obtain "explicit consent" from the client to use this information. The Money Advice Liaison Group have produced a Briefing Note that explains what explicit consent involves:

1. Fully explaining to individuals why their information is being collected, how it will be used to help decision-making, and who (if anyone) the data will be shared with/disclosed to.
2. Asking individuals whether they understand this explanation, and whether they consent or agree to continue with the processing of their data

Releasing information to detect or prevent a crime

From time to time CAP may receive requests from the police or other organisations (such as local

authority or HMRC fraud investigation units) for the disclosure of information relating to a client(s) that is required in connection with the prevention or detection of a crime, the apprehension or prosecution of offenders, or the assessment or collection of tax - this is commonly known as a section 29 request as it refers to section 29 of the Data Protection Act, this section allows for information to be shared without the consent of the data subject. Whilst in most cases it is likely to be in the public interest to assist such bodies by providing the required information, CAP is committed to ensuring that all such disclosures are fair and lawful, and in particular, that they are compliant with the Data Protection Act. We would expect, in most cases, that the request will be received at head office but if you receive such a request directly then you should forward it to either The Data Protection Officer or the Quality Assurance Officer at head office for them to deal with the request for disclosure.

## Data Protection Breach Protocol

### What Constitutes a Data Breach?

For a data breach to attract a monetary penalty the Information Commissioner must be satisfied that there has been a serious breach, that it was likely to cause damage or distress, that it was either deliberate or negligent and that the organisation failed to take reasonable steps to prevent it.

Examples given by the ICO are as follows:

Damage; - Following a security breach, financial data is lost and a client becomes a victim of identity fraud.

Distress; - Following a security breach, details relating to the health issues of a client are stolen and an individual suffers worry and anxiety that their sensitive personal data will be made public, even if these concerns do not materialise.

Deliberate; - A marketing company collects personal data stating it is for the purpose of a competition and then, without consent, knowingly discloses the data to populate a tracing database for commercial purposes without informing the individuals concerned.

Reputational Damage; - Even if a fine is not imposed, a data security breach can cause reputational damage to the charity and possible loss of confidence by our clients, referrers, supporters, creditors and the Christian community at large.

### What situations could constitute a data breach?

A data breach would be caused when, but not limited to:

- An overheard conversation about a client or someone being able to view data about a client on your computer screen.
- A laptop or other device containing unencrypted personal data is lost or stolen
- Personal data is stored on a personal computer at the home of a staff member and access to the computer is subsequently 'blagged' – where information is obtained by deception – or the computer is sold but the hard drive was not irretrievably deleted and the personal data is potentially stolen or lost
- An unencrypted USB (memory stick) containing personal data is lost or stolen
- Paper files containing personal data are lost or stolen
- An email is sent (either internally or externally) with files attached containing personal data and the email is sent to the wrong email address
- An email is sent (either internally or externally) with files attached that contain personal data that is far in excess of that necessary in order for the business function to be carried out
- An email is sent (either internally or externally) which should have been sent 'bcc' to a large number of supporters, is instead, sent 'to' and so each recipient is aware who else has received the email, their personal email address and potentially other personal details
- We become aware that personal data that has been shared outside of the charity for a legitimate charitable purpose has been lost by the recipient, stolen from the recipient, or is used by the recipient in a manner for which they have no authority
- Personal data is transferred electronically outside of the charity and is not encrypted as it should be

- Paper files of personal data are left unattended and are taken or copied and then used for an unauthorised purpose
- A member of staff or volunteer uses personal data for a personal rather than a Charity reason.

## What to do when a Data Breach Occurs

### Reporting of the breach

If it is found, or suspected that a data security breach has taken place, an appropriate member of staff must be informed immediately.

The person who discovers the data security breach must immediately inform the IT Helpdesk – the number to call is 01274 760781. Once IT has been notified, they can decide the best response but in the case of a computer/tablet/phone breach, the affected device should be turned off and disconnected from the Internet immediately.

The IT Helpdesk will act as primary contact and should be given the following information:

- What data was involved?
- Was the data encrypted or password protected?
- Who are the individuals potentially affected?
- Full and accurate details of the incident, including who is reporting the incident, when it occurred, the location, and attempts already made to recover the data.

If the breach is discovered outside of normal office hours, this should be reported as soon as is practicable.

Once the breach has been reported, CAP will initiate its Data Protection Breach Protocol which may involve informing the ICO of the data breach and will involve informing the individuals affected that their data has been compromised – clients can then take appropriate action to protect their information and interests.

## Confidentiality policy

Christians Against Poverty is committed to providing a confidential advice service to its clients. We believe that principles of confidentiality must be integrated across all aspects of services and management. We believe our clients deserve the right to confidentiality to protect their interests and safeguard Christians Against Poverty's services.

We understand confidentiality to mean that no information regarding a client shall be given directly or indirectly to any third party that is external to the Agent, staff and manager, without that client's prior expressed consent to disclose such information.

We also expect an Agent to conform to any confidentiality policies held by their church.

Additionally, a client's identity/case details should not be passed to any other Agents or members of staff except in situations necessary to complete a task properly and when it is in the best interests of the client (e.g. referring a case for approval). It is not permitted for anyone to access a client's details except in the normal course of carrying out duties.

An Agent should recognise that all clients should be able to access Christians Against Poverty's services in confidence and that no other person should ever know that they have used our services without the client's consent.

Agents should recognise that clients need to feel secure in using CAP's services in a confidential manner. Then should ensure all clients are afforded confidential interview space (if it is required). They should not confirm the client's presence in the centre or use of the centre without obtaining the client's consent.

CAP is responsible for the safe handling of personal data and confidential information relating to both

CAP and our clients. This includes information held, received or transmitted in both writing and verbal form, and information that is electronically stored and physically held. CAP is also responsible for ensuring that its computer-based systems are used securely.

As an Agent you agree to meet the following requirements at all times.

#### **Confidential information relating to CAP**

Confidential information in this context includes, but is not limited to:

- Any information relating to CAP (including any CAP derivative services, such as CAP Money, CAP Job Clubs, etc.) that is not publicly known or which CAP has not disclosed to the general public
- Any information relating to CAP's internal policies, procedures and systems
- Contact details (including postal and electronic mail addresses, telephone and fax numbers) of staff and creditors – except where this is already accessible to the public.

You must not disclose confidential information relating to CAP to any third party.

#### **Confidential information relating to clients**

Confidential information in this context includes, but is not limited to:

- Any personal data as defined by s.1(1) Data Protection Act 1998
- Contact details (including postal and electronic mail addresses, telephone and fax numbers) of clients
- Personal details (including dates of birth, national insurance details and other information by which a living individual can be identified) relating to clients
- Financial details (including any information relating to income and debts) of clients
- Any information recorded in casenotes, irrespective of how they were generated
- Any personal information recorded or communicated in any form for which we do not have the client's prior consent.

Agents must not access confidential information relating to clients unless such access is necessarily made in the proper course of your work with CAP. Any paperwork an Agent has been given by a client must be handled and stored securely until it is posted to head office, and the Agent should not retain it longer than necessary.

Agents must not disclose confidential information relating to clients to any third party, except to the extent that such disclosure is necessarily made in the proper course of their work with CAP. This should only be done once permission has been obtained from their CAP Line Manager or a member of staff.

### **Statistical recording**

Christians Against Poverty is committed to effective statistical recording to enable us to monitor take-up and effectiveness of our service and to identify any policy issues arising from our advice services.

It is the relevant head office manager's responsibility to ensure that all statistical records given to third parties, such as to support funding applications or monitoring reports for the local authority are produced in anonymous form.

### **Support Team Volunteers**

Centre Managers and Debt Coaches are responsible for ensuring that Support Team Volunteers 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 at [https://documents.cap-systems.org/Debt\\_Centres/Debt\\_Centre\\_Support\\_Teams](https://documents.cap-systems.org/Debt_Centres/Debt_Centre_Support_Teams)

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 on a filing cabinet in the office – Area Managers will

check this data annually and Regional Managers will check on the accompanied 3-month visit to ensure compliance.

### Case records

All case records must be locked away at the end of each working day. All information relating to clients will be left in locked drawers. Records should only be kept until the relevant Debt Ops team has confirmed receipt of them and then should be securely destroyed.

### Expressed consent to give information

It is the responsibility of an Agent to ensure that where Christians Against Poverty agrees any action on behalf of a client, that client must first sign an authorisation form. This should be sent to head office to be placed in the client's file.

All staff should take reasonable steps to ensure that they are speaking with the correct client to maintain anonymity when making contact with clients. Until this check has been made with clients, all staff must ensure they make no reference to Christians Against Poverty when making telephone contact with clients. Agents are responsible for checking with clients if it is acceptable to call and write to them at home or work in relation to their case.

All details of expressed consent must be recorded on the case file.

### Breaches and limits of confidentiality

Limits to confidentiality occurs as it is widely accepted that we have a general obligation to warn or protect people whom a client places in imminent harm, the right of the client to confidentiality is therefore balanced by the need to ensure the safety of others – for instance a safeguard and limit to confidentiality would be a strong suspicion that there is a case of child abuse or neglect.

Balancing the relationship with the protection of at-risk populations is complex and emotionally charged but clear policies and procedures make dealing with these issues easier to deal with and empower you, as our Agent and your support team volunteers, to instigate the appropriate action.

We recognise that occasions may arise where an individual Agent or support team volunteer feel they need to breach confidentiality. We also recognise, however, that any breach of confidentiality may damage the reputation of our services and therefore has to be treated very seriously. Please be aware that if challenged, an Agent must be prepared to defend their decision to the Information Commissioners Office (ICO) or in court as the Data Protection Act still applies. CAP advises Agents to ensure that any such decisions are taken at an appropriately senior level (see specific guidance that follows) within CAP and that the reasons for the decision are documented. If an Agent feels confidentiality should be breached, the following steps must be taken:

1. The Agent should raise the matter immediately with their CAP Line Manager
2. The Agent should discuss with their CAP Line Manager the issues involved in the case and explain why they feel confidentiality should be breached and what would be achieved by breaching confidentiality. The CAP Line Manager will take a written note of this discussion.
3. The CAP Line Manager is responsible for discussing with the Agent what options are available in each set of circumstances.
4. The CAP Line Manager is responsible for making a decision on whether confidentiality should be breached. If the CAP Line Manager decides that confidentiality is to be breached then they should contact one of the Debt Ops Team Managers and brief them on the full facts of the case, ensuring they do not breach confidentiality in doing so. They should then seek authorisation to breach confidentiality from them.

If the Debt Ops Team Manager agrees to a breach of confidentiality, a full written report on the case should be made and any action agreed undertaken. The CAP Line Manager is responsible for ensuring all activities are taken.

If the Debt Ops Team Manager does not agree to breach confidentiality, this is the final decision of Christians Against Poverty.

In no circumstances should any breach of confidentiality be discussed at this stage with any other member of the senior management team or management board. This is to ensure that any future complaints or investigations arising from breach in confidentiality can be carried out in an independent manner.

#### Legislative framework

Christians Against Poverty will monitor this policy to ensure it meets statutory and legal requirements including the Consumer Credit Regulations under the FCA, Data Protection Act, Children's Act, Rehabilitation of Offenders Act and Prevention of Terrorism Act. Training will include these aspects.

#### Ensuring the effectiveness of the policy

All management board members will receive a copy of the confidentiality policy. Existing and new caseworkers, Centre Managers and Debt Coaches will be introduced to the confidentiality policy via induction and training.

The policy will be reviewed annually and amendments should be proposed and agreed by the Head of HR and the senior management team.

#### Privacy policy

CAP's privacy policy is published on CAP's website and covers all CAP's derivative names and services which are part of the CAP franchise and brand. It tells anyone accessing and/or supporting our charity what to expect when Christians Against Poverty collects personal information. It applies to information we collect about:

- Visitors to our websites
- Complainants
- People who use our services – clients, supporters, etc.
- Job applicants and our current and former employees and Agents.

Christians Against Poverty will, from time-to-time, make changes to this statement by updating this page on our website. Agents are advised to check regularly to see what has changed and to ensure that they are happy with any changes.