Care4Calais Data Protection Policy

Prepared by: Clare Moseley

Owned by: Alex Clegg

Policy review date: 27 February 2024

Contents

1. OBJECTIVE

1.1 Care4Calais takes data protection seriously and seeks to ensure that Personal Data is processed fairly, lawfully and in compliance with the applicable data protection laws.

1.2 This Data Protection Policy (**"Policy"**) seeks to provide general overarching guidelines to ensure that Care4Calais is aware of its data protection compliance obligations. It is not intended as a definitive statement of the application of all applicable data protection laws; instead, it acts as a general framework of best practice, setting out the principles of data protection adopted within Care4Calais.

1.3 Any breach of this policy will be taken seriously and may result in disciplinary action.

2. SCOPE

2.1 It is the responsibility of all our staff, which includes volunteers and employees ("**Staff**"), to assist Care4Calais to comply with this Policy. Our volunteers must comply with the parts of the policy which apply to them.

2.2 The types of information that Care4Calais handles include details of current, past and potential service users who are asylum seekers ("**Service Users**"); current, past and prospective Staff; and others that we communicate with.

2.3 The Policy covers all Personal Data in any form, including but not limited to electronic data, paper documents and disks and all types of Processing, whether manual or automated that is under Care4Calais' possession or control. This will include information held about Care4Calais Staff, Service Users and business contacts.

2.4 This policy sets out Care4Calais' rules on data protection and the legal conditions that must be satisfied in relation to the obtaining, handling, processing, storage, transportation and destruction of personal information.

2.5 This policy does not form part of any employee's contract of employment and may be amended at any time.

3. DEFINITIONS

3.1 **Service Partner** shall mean a third party who receives personal data from Care4Calais, or who processes personal data on behalf of Care4Calais for example local authorities, and suppliers and other service providers. This includes lawyers, Migrant Help, and the Home Office.

3.2 **Data Subject** shall mean an identified or identifiable person whose Personal Data is being processed.

3.3 **Informed Consent** shall mean any freely given specific and informed indication of the Data Subject's agreement to the Processing of his/her Personal Data.

3.4 **Personal Data** shall mean any information capable of identifying a natural person, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to their physical, physiological, mental, economic, cultural or social identity. Data is considered personal when it enables anyone to link information to a specific person, even if the person or entity holding that data cannot make that link.

3.5 **Processing** shall mean any operation or set of operations that is performed upon Personal Data, whether or not by automatic means, including, but not limited to collection, recording, organisation, storage, access, adaptation, alteration, retrieval, consultation, use, disclosure, dissemination, making available, alignment, combination, blocking, deleting, erasure, or destruction (and Process shall be interpreted accordingly).

3.6 **Staff** shall include all Care4Calais employees and volunteers and includes temporary and permanent employees.

4. LEGAL COMPLIANCE

Care4Calais complies with the data protection laws of the UK, including with policies and codes of conduct issued by regulators such as the Information Commissioner's Office and the Charity Commission.

5. DATA PROTECTION REQUIREMENTS

The following requirements set out how Personal Data should be treated:

5.1 **Notice to Data Subjects - Data Subjects must be informed about the types of data collected, the purposes for which the data are collected, and anyone to whom their Personal Data may be disclosed outside of Care4Calais (e.g., Service Partners).**

5.1.1 This requirement will be satisfied by issuing a privacy notice to Data Subjects at the point where Personal Data are originally collected from them, or as soon as possible thereafter. Specifically, Service Users are provided with a short form, plain English privacy notice at the point at which they first engage with Care4Calais. Staff should be prepared to answer questions about this privacy notice and explain to Service Users how and why their Personal Data is collected and used by Care4Calais. In addition, all Staff will receive a privacy notice explaining how Care4Calais uses their Personal Data to recruit them as volunteers / employees, and to manage their ongoing relationship with Care4Calais as either a volunteer or employee.

5.1.2 Privacy notices shall be written in language which provides Data Subjects with a clear understanding as to how their Personal Data will be used, with particular emphasis on any unusual aspects of Processing. For example, where fundraising communications will be sent to supporters, the Data Subject must be made aware in advance of what form this will take and how they can opt out of such communications.

5.1.3 Care4Calais' "Service User Privacy Notice" and "Employee and Volunteer Privacy Notice" can be requested from alexander@care4calais.org.

5.2 **Fair Processing - The way in which Personal Data is held and used must be kept consistent with the privacy notice provided to the Data Subject.**

5.2.1 Personal Data should be used only as anticipated in the original privacy notice. No further or alternative use should be made of the Personal Data without considering the need to obtain informed consent from the Data Subject and/or issuing an updated privacy notice.

5.2.2 The data subject must be told who the data controller is, in this case Care4Calais, the purpose for which the data is to be processed, and the identities of anyone to whom the data may be disclosed or transferred.

5.2.3 Data about Service Users will be processed to help them complete their asylum application and to find accommodation and support for them. Care4Calais has a legitimate interest in helping Service Users in this way, and the processing of Personal Data is necessary to satisfy this purpose. It may be necessary for Care4Calais to also process sensitive Personal Data of Service Users for these purposes – for example, health, race or religion data relevant to an asylum application. Care4Calais will process this data on the following basis:

- UK GDPR Article 9(2)(g) – where processing is necessary for reasons of substantial public interest, specifically for the safeguarding of children and of individuals at risk (Schedule 1, Part 2, section 18, DPA 2018).

5.2.4 Data about Staff may be processed for legal, personnel, administrative and management purposes and to enable the data controller to meet its legal obligations as an employer, for example to pay Staff, monitor their performance and to confer benefits in connection with their employment. Examples of when sensitive personal data of Staff is likely to be processed are set out below:

5.2.4.1 information about a Staff's physical or mental health or condition in order to monitor sick leave and take decisions as to the employee's fitness for work;

5.2.4.2 conducting criminal record checks where these are required or expressly authorised by law (e.g. for those working with vulnerable persons or in finance roles), or the handling of criminal offence information in the context of attachment from earnings orders;

5.2.4.3 the employee's racial or ethnic origin or religious or similar information in order to monitor compliance with equal opportunities legislation; and

5.2.4.4 in order to comply with legal requirements and obligations to third parties.

5.3 **Proportionality - The nature and type of Personal Data held must be proportionate and necessary for the purpose for which it is to be required.**

5.3.1 There should be a clear justification which accords with the aims of the charity, or otherwise a legal requirement to hold the specific types of Personal Data that are collected from individual Data Subjects. Care must be taken to avoid collecting excessive or irrelevant elements of Personal Data or allowing Personal Data to be used for purposes that cannot be justified as 'necessary'. If this test cannot be satisfied, then it may be unlawful to collect the Personal Data without Informed Consent from the Data Subject.

5.3.2 For example, when collecting Personal Data as part of the recruitment process, the only categories of Personal Data which should be collected are those necessary to allow the selection of Staff, the conduct of vetting processes, and the population of initial employment records.

5.3.3 Personal Data should not be collected for one purpose and then used for another. If it becomes necessary to change the purpose for which the data is processed, the Data Subject should be informed of the new purpose before any processing occurs.

5.4 **Sharing Personal Data outside Care4Calais - Personal Data should only be disclosed outside Care4Calais where there is a legitimate charitable need, or an overarching legal requirement to do this.**

5.4.1 Disclosure must be made on a strictly limited 'need to know' basis where there is clear justification for transferring Personal Data - either because the Data Subject has consented to the transfer or because it is for a legitimate charitable need. In each case the Data Subject must be aware that the transfer is likely to take place. Assurances should also be sought from the recipient that they will only use the Personal Data for legitimate / authorised purposes and keep it secure.

5.4.2 If a particular disclosure is required to meet a legal or regulatory obligation (for example to a government agency, a regulator (e.g., the ICO or Charities Commission or police force / security service) or in connection with legal proceedings, the Personal Data may be provided so long as the disclosure is limited to that which is legally required. Where permitted by law, the Data Subject should also be made aware of the situation (i.e., the Data Subject was told about the possibility of a disclosure in the privacy notice and is then notified specifically at the time of the actual request for disclosure).

5.5 **Transferring Personal Data Overseas**

5.5.1 Particular care must be taken about transferring Personal Data to any country or territory outside the United Kingdom and the European Economic Area ('EEA'). Generally, a mechanism must be in place for ensuring an adequate level of protection for Personal Data transferred to a 'third country'. For example, Care4Calais may need to enter into the ICO's 'International Data Transfer Agreement' with any Service Partner located in a third country.

5.5.2 Be aware that transfers may take place that are not obvious (e.g., if a service provider that we have appointed in the UK sub-contracts some of its Processing obligations to a company in India there will be a transfer of data out of the UK/EEA (from the service provider to the sub-contractor) which will be prohibited unless certain conditions are met).

5.6 **Accuracy - Personal Data should be archived, cleansed and deleted after appropriate periods of time.**

5.6.1 Personal Data must be kept accurate, complete and up-to date and not retained for longer than the purposes for which it was collected unless there is a clear overriding charitable or business need or legal / regulatory requirement to retain the Personal Data.

5.6.2 Information which is incorrect or misleading is not accurate and steps will need to be taken to check the accuracy of any personal data at the point of collection and at regular intervals afterwards. Inaccurate or out-of-date data must be destroyed.

5.7 **Rights of Data Subjects - Data Subjects generally have the ability to have access to their Personal Data on request and may also be entitled to prevent or challenge the Processing of their Personal Data or have it deleted. Data subjects also have an unconditional right to prevent (i.e., opt-out of) direct marketing at any time.**

5.7.1 Data Subjects must be provided with the opportunity to access their Personal Data at reasonable intervals for the purposes of examining it, confirming its accuracy and amending it if it is incomplete or inaccurate.

5.7.2 In privacy notices, Data Subjects should be provided with contact information to enable them to exercise their rights.

5.7.3 Requests by a Service User or member of Staff to amend inaccurate contact details or biographical information may be dealt with by an appropriate member of Care4Calais Staff. All other requests from Data Subjects to exercise rights should be notified to alexander@care4calais.org.

5.7.4 Except where the identity of a requester is certain (for example, a request is made by an existing employee from a Care4Calais email address), steps should be taken to confirm the identity of the requester, by asking for proof of identity documentation (e.g., a passport or driving licence). Care4Calais will have one month from the date of a request (or the date on which proof of identity is received) to issue its

response, except where the request is particularly onerous, and an extension of up to two months can be permitted.

5.8 **Security of Personal Data - Appropriate technical and organisational security measures must be taken to prevent unauthorised or unlawful disclosure or access to, or accidental or unlawful loss, destruction, alteration or damage to Personal Data.**

5.8.1 All Staff who have access to Personal Data are under a legal responsibility to keep information confidential. Access and use of Personal Data must be limited on a strict 'need to know' basis.

5.8.2 Where Personal Data is passed to a Service Partner, assurances should be sought about the appropriate purposes for which the Service Partner will Process the Personal Data, and their commitment to comply with data protection laws. Where a Service Partner processes Personal Data on behalf of Care4Calais under its instructions (e.g., supplier such as a data hosting provider, payroll processor or marketing automation provider) that Service Partner must enter into a written agreement with Care4Calais that contains 'data processing terms' (as required by Article 28(3) of the UK GDPR).

5.8.3 Care4Calais is required to put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction.

5.8.4 Maintaining data security means guaranteeing the confidentiality, integrity and availability of the personal data, defined as follows:

5.8.4.1 **Confidentiality** means that only people who are authorised to use the data can access it.

5.8.4.2 **Integrity** means that personal data should be accurate and suitable for the purpose for which it is processed.

5.8.4.3 **Availability** means that authorised users should be able to access the data if they need it for authorised purposes. Personal data should therefore be stored on our central computer system instead of individual PCs.

5.8.5 Security procedures include:

5.8.5.1 **Entry controls.** Any stranger seen in entry-controlled areas should be reported.

5.8.5.2 **Secure lockable desks and cupboards.** Desks and cupboards should be kept locked if they hold confidential information of any kind. Personal information is always considered confidential.

5.8.5.3 **Methods of disposal.** Paper documents should be shredded. Physical storage media should be physically destroyed when they are no longer required.

5.8.5.4 **Equipment.** Data users should ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC when it is left unattended.

5.8.5.5 **Back-up.** Care4Calais should be able to restore the availability of personal data which is lost or deleted. Therefore, files containing personal data should be backed-up appropriately.

5.8.5.6 **Password protection.** Electronic documents containing substantial amounts of personal data (for example, a spreadsheet of supporters or payroll information) should be password protected, and the password should be circulated in a separate email from the email attaching the document.

5.9 **Data Breaches - All losses of Personal Data should be contained and remedied as soon as possible and where necessary all appropriate stakeholders informed of the data breach.**

5.9.1 A Data Breach is an incident which involves an unauthorised or inappropriate disclosure of, or access to, Personal Data. Some examples of data breaches include: third party attacks on IT infrastructure designed to harvest personal data for criminal purposes; accidental loss or theft of Care4Calais devices (e.g., mobile phones, laptops, USB devices); the passing to third parties or disposal of personal information without appropriate security measures being in place.

5.9.2 All Staff have an obligation to report data breaches (or suspected data breaches) to alexander@care4calais.org immediately. Care4Calais is subject to a statutory obligation to report most breaches within 72 hours of becoming aware that a breach has occurred.

5.10 **Direct marketing - Before using Personal Data for direct marketing purposes, ensure the Data Subject has given appropriate consent to use their details in this way.**

5.10.1 Some form of consent will be required from Data Subjects, who also should have been provided with a standard data protection notice and a clear link to the relevant Care4Calais Privacy Policy.

5.10.2 Data Subjects must be given the chance to decline to receive direct marketing material (both when details are collected and at any point thereafter) and a suppression list should be held listing Data Subjects who have indicated that they do not want to be contacted in the future.

5.11 **Cookies**

5.11.1 The Care4Calais website should not deploy cookie technology without having a clear statement explaining to users how cookies are deployed and giving individuals an opportunity to consent before having cookies placed on their computers.

5.12 **Automated decision-making - Decisions should not be made about individuals using entirely automated Processes.**

5.12.1 Advice should be sought from alexander@care4calais.org before considering any techniques that will result in decisions being made about individuals through automated means (for example, automated screening processes used during recruitment), to ensure appropriate manual reviews are embedded into the decision-making Process.

5.13 **CCTV - CCTV systems should be operated with care to avoid disproportionate risk of privacy intrusion to individual Data Subjects.**

5.13.1 CCTV systems should be installed and operated in a way that is proportionate to the risks being covered and prominent notices should be displayed in the area covered by the CCTV system to make sure people are aware that the system is in operation.

6. CRIMINAL OFFENCES

6.1 The following constitute criminal offences which may be committed by any member of Care4Calais Staff in connection with the handling of Personal Data:

6.1.1 deliberately or recklessly deleting Personal Data which forms part of a request from a Data Subject to access that data (after the request has been made, but before the data has been provided to the requester);

6.1.2 deliberately or recklessly obtaining, disclosing or holding on to personal data without the approval of Care4Calais;

6.1.3 deliberately or recklessly re-identifying anonymised data.

7. PROVIDING INFORMATION TO THIRD PARTIES

7.1 Any member of Staff dealing with enquiries from third parties should be careful about disclosing any personal information held by us. In particular they should:

7.1.1 check the identity of the person making the enquiry and whether they are legally entitled to receive the information they have requested;

7.1.2 suggest that the third party put their request in writing so the third party's identity and entitlement to the information may be verified;

7.1.3 refer to their line manager for assistance in difficult situations; and

7.1.4 where providing information to a third party, do so in accordance with the eight data protection principles.

8. CONSEQUENCES OF NON-COMPLIANCE

8.1 If Care4Calais is found to be in breach of applicable data protection legislation, data protection supervisory authorities may:

8.1.1 impose monetary penalties; or

8.1.2 issue other enforcement proceedings against Care4Calais which could result in:

8.1.2.1 further use of the affected Personal Data being prevented; or

8.1.2.2 Care4Calais being required to change its processing procedures, or having other conditions imposed upon it in respect of the Processing of Personal Data.

8.2 Enforcement action will usually have a cost and time implication for the charity. However, more damaging might be any restrictions imposed upon us which prevent Care4Calais from exploiting our databases for fund raising purposes.

8.3 Additionally, the associated publicity could make Care4Calais appear as an organisation that does not respect the privacy rights of individuals and cause reputational damage to Care4Calais. The charity sector has been under the spotlight in terms of data protection and direct marketing issues, and we can expect close attention from the press and from our regulators if anything goes wrong.

9. ACCOUNTABILITY FOR OUR ACTIONS

9.1 Periodic monitoring of adherence to this Policy takes place to help ensure compliance with this Policy, applicable laws and/or contractual agreements in connection with the handling of Personal Data.

9.2 It is the responsibility of all our Staff to assist Care4Calais to comply with this Policy. All Staff must familiarise themselves with both this Policy and apply their provisions in relation to all processing of Personal Data. Failure to do so could amount to misconduct, which is a disciplinary matter and could ultimately lead to dismissal.

10. ENFORCEMENT AND COMPLAINTS PROCEDURE

10.1 Care4Calais is committed to resolving the legitimate privacy issues of its Staff, customers and other contacts. If a member of Staff feels that he/she has done something in breach of this Policy, they must contact Finance and report the matter. The failure to report a breach will likely lead to more serious consequences than reporting the matter.

10.2 Members of Staff may also confidentially submit good faith complaints regarding violations of this Policy or any other data protection breach to alexander@care4calais.org. In order to submit a complaint, members of Staff should contact alexander@care4calais.org to confidentially explain and review the matter.

10.3 If an individual covered by this Policy makes a complaint about the Processing of his/her or someone else's Personal Data, and the complaint is not satisfactorily resolved through this internal procedure, Care4Calais will co-operate with the appropriate data protection authorities and comply with the advice of such authorities to resolve any outstanding complaints. In the event that the data protection authorities determine that Care4Calais or one or more of its Staff failed to comply with this Policy or the data protection laws, upon recommendation of the authorities, Care4Calais will take appropriate steps to address any adverse effects and to promote future compliance.

11. FURTHER GUIDANCE AND QUERIES

11.1 Further guidance on data protection compliance is available in the linked policies and checklist documents.

11.2 If you have any queries, please speak in the first instance to alexander@care4calais.org

12. UPDATES

12.1 The current version number of this document is shown on page 1. This Policy is reviewed annually by Alex Clegg and Clare Moseley to ensure it is achieving the stated objectives. Any variations to this Policy will be shared with Staff.