Data Protection/GDPR Policy

Policy Statement

Cloudy Foundation is fully committed to compliance with the requirements of the Data Protection Act 1998 (DPA). We are required to maintain certain personal data about individuals for the purposes of satisfying our operational and legal obligations. We recognise the importance of correct and lawful treatment of personal data as it helps to maintain confidence in our charity and to ensure efficient and successful outcomes when using this data.

Cloudy Foundation is committed to ensuring that all personal information handled by us will be processed according to legal compliant standards of data protection and data security.

Purpose

The purpose of this policy is to ensure that everyone working with Cloudy Foundation, and all partners and associates, including volunteers, is aware of the responsibilities they and others have in relations to data protection issues.

This policy sets out clear guidance for the acceptable handling and transmission of data and ensures the confidentiality and of all charity staff and volunteers is maintained at all times.

It also ensures that all staff and volunteers understand the consequences of not complying with this policy.

The further purpose of this policy is to help us achieve our data protection and data security aims by:

a. Setting out how the Charity uses and protects any personal information that we may hold about individuals
b. Ensuring our staff understand our rules and the legal standards for handling personal information relating to staff and others
c. Clarifying the responsibilities and duties of staff in respect of data protection and data security.

We may amend this policy at any time, at our discretion

Principles

Maintaining appropriate standards of data protection and data security is a collective task shared between the Charity and the staff. This policy and the rules contained in it apply to all staff of the Charity, irrespective of seniority, tenure and working hours, including all employees, directors and officers, consultants and contractors, casual or agency staff, trainees, homeworkers and fixed-term staff and any volunteers.

David Hall, Chair of Trustees is appointed as the Data Protection Officer and has overall responsibility for ensuring that all personal information is handled in compliance with the law.

All Staff have personal responsibility to ensure compliance with this policy, to handle all personal information consistently with the principles set out here and to ensure that measures are taken to protect the data security. Managers have special responsibility for leading by example and monitoring and enforcing compliance.

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

We endorse and adhere to the eight principles of the Data Protection Act which are summarised as follows:
Data must:
1. be processed fairly and lawfully and shall not be processed unless certain conditions are met.
2. be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose.
3. be adequate, relevant and not excessive for those purposes.
4. be accurate and, where necessary, kept up to date.
5. only be kept for as long as is necessary for the purpose for which it was obtained.
6. be processed in accordance with the data subject's rights.
7. be kept secure from unauthorised or unlawful processing and protected against accidental loss, destruction or damage by using the appropriate technical and organisational measure.
8. not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.
These principles apply to obtaining, handling, processing, transportation and storage of personal data. Staff and agents of Cloudy Foundation who obtain, handle, process, transport and store personal data for us must adhere to these principles at all times.
It should be noted that information shared with employees/volunteers of the charity in the pursuance of its aims and mission, whether by individuals, organisations and other agencies, including staff and volunteers, is confidential to the charity and not to the individual with whom it was shared.

Processes

1. Handling of personal/sensitive information – see also Personal information and activities covered by this policy

This policy covers personal information:

a. Which relates to a living individual who can be identified either from that information in isolation or by reading it together with other information we possess
b. Is stored electronically or on paper in a filing system
c. In the form of statements of opinion as well as facts
d. Which relates to Staff (present, past or future) or to any other individual whose personal information we handle or control
e. Which we obtain, hold or store, organise, disclose or transfer, amend, retrieve, use handle process, transport or destroy.

Cloudy Foundation will, through appropriate management and the use of strict criteria and controls:
a. observe fully the conditions concerning the fair collection and use of personal information
b. specify the purpose for which information is used
c. collect and process information only to the extent that it is needed to fulfil operational needs or legal requirements
d. endeavour always, to ensure the quality of information used
e. not keep information for longer than required, operationally or legally
f. always endeavour to safeguard personal information by physical and technical means (i.e. keeping paper files and other records or documents containing personal/sensitive data in a secure environment; protecting personal data held on computers and computer systems by the use of secure passwords, which where possible, are changed periodically and ensuring that individual passwords are not easily compromised)
g. ensure that personal information is not transferred abroad without suitable safeguards
h. ensure that the lawful rights of people about whom the information is held can be fully exercised.
In addition, Cloudy Foundation will ensure that:
i. there is someone with specific responsibility for data protection for the charity (the designated Data Controller) - currently the Chair of Trustees.
j. all those who manage and handle personal information understand that they are contractually responsible for following good data protection practice
k. all those who manage and handle personal information are appropriately supervised and trained to do so
l. a clear procedure is in place to deal with any data access requests (internal or external) that ensures that such enquiries are dealt with promptly and courteously
m. methods of handling personal information are regularly assessed and evaluated
n. any data sharing is carried out under a written agreement, setting out the scope and limits of the sharing
o. any disclosure of personal data will be in compliance with approved procedures.

Staff whose work involves using personal data must comply with this policy and with the legal data protection principles which require that personal information is:

a. Processed fairly and lawfully. We must always have a lawful basis to process personal information. In most (but not all) cases, the person to whom the information relates (the Subject) must have given consent. The Subject must be told who controls the information (us), the purpose(s) for which we are processing the information and to whom it may be disclosed.
b. Collected for specified, explicit and legitimate purposes. Personal information must not be collected for one purpose and then used for another. If we want to change the way we use personal information, we must first tell the Subject.
c. Adequate, relevant and limited to what is necessary.
d. Accurate and kept up to date. Regular checks must be made to correct or destroy inaccurate information.
e. Kept for no longer than is necessary. Information must be destroyed or deleted when we no longer need it. For guidance on how long particular information should be kept, contact the Data Protection Officer.
f. Processed in a manner that ensures appropriate security. See section on data security below.

Data subjects' rights

The Charity will process personal data in line with data subjects' rights. Data subjects have the right to:

a. Be informed. About the identity and contact details of the controller/processor, the purpose and/or legal basis for processing the data, how the data is to be processed, how long the data will be kept, which parties are involved in the processing of data and the privacy policy of the controller/processor.
b. Access. There must be a Subject Access Request process so that Subjects may request a copy of their data.
c. Rectify incorrect personal information. Subjects must have a facility to request that incorrect information is corrected.
d. Be forgotten. Subjects may withdraw consent and ask for personal information to be erased. There are certain exemptions to this (e.g. employees)
e. Request their data be moved. Subjects can request that their data be moved elsewhere (e.g. to a competitor).
f. Object. Subjects must be allowed to object to their personal information being processed. They must be able to opt-out if their personal information is being processed based on legitimate interests, the public interest, exercise of official authority, for direct marketing and for purposes of scientific/historical research and statistics.
g. Restrict processing of their data. When processing is restricted, storage of the data is permitted, but further processing is not.

h. Not have their data used for automated decision making and profiling. Such processing must have specific consent, be necessary for the performance of a contract or must be authorised by law.

2. Access to personal data

All individuals who are the subject of personal data held by us are entitled to:
a. ask what information we hold about them and why
b. ask how to gain access to it
c. be informed of how to keep it up to date
d. have inaccurate personal data corrected or removed
e. prevent us from processing information or request that it is stopped if the processing of such data is likely to cause substantial, unwarranted damage or distress to the individual or anyone else
f. require us to ensure that no decision which significantly affects an individual is solely based on an automated process for the purposes of evaluating matters relating to him/her, such as conduct or performance
g. be informed what we are doing to comply with our obligations under the Data Protection Act.
This right is subject to certain exemptions which are set out in the Act.

3. Data Subject Access Request

Any person who wishes to exercise the right to access their information should make a request in writing, to the Chair of Trustees. A fee of £10.00 is payable for each subject access request. If personal details are inaccurate, they will be amended upon request. If by providing this information we would have to disclose information relating to or identifying a third party, we will only do so provided the third party gives consent, otherwise we may edit the data to remove the identity of the third party.
Unless we are under a legal obligation to release data, or the individual has given us permission, personal information will only be released to the individual to whom it relates. The disclosure of such information to anyone else without their consent may be a criminal offence. Any staff member who is in doubt regarding a subject access request should check with the Chief Executive.
Information must under no circumstances be sent outside of the UK without the prior permission of the Chair of Trustees.
We aim to comply with requests for access to personal information as quickly as possible, but will ensure that this is provided within 40 days of receipt of a written request unless there is good reason for delay. In such cases, the reason for the delay will be explained in writing to the individual making the request.

Subject access requests

By law, any Subject (including Staff) may make a formal request for information that we hold about them, by completing a Subject Access Request (SAR). If you would like a copy of the information we hold on you please write to us at at the address below.

If you believe that any information we are holding on you is incorrect or incomplete, or if you wish to have it deleted, please write to us at the address detailed below. We will correct any information found to be incorrect or delete it if requested.

In the case of Staff, we will only delete the information once the employment or engagement has ceased and it is no longer required to comply with our legal obligations, assist in a criminal investigation or for legal and regulatory authorities, such as HM Revenue and Customs.

Any member of Staff who receives such a request from a third party should forward it to the Data Protection Officer immediately.

Data security

We must all protect personal information in our possession from being accessed, lost deleted or damaged unlawfully or without proper authorisation through the use of data security measures.

Maintaining data security means making sure that:

a. Only people with are authorised to use the information can access it
b. Information is accurate and suitable for the purpose for which it is processed
c. Authorised persons can access information if they need it for authorised purposes. Personal information therefore should not be stored on individual computers but instead on our central system.

By law, we must use procedures and technology to secure personal information throughout the period that we hold or control if, from obtaining to destroying the information.

Personal information must not be transferred to any person to process (e.g. while performing services for us or on our behalf) unless that person has either agreed to comply with our data security procedures, or we are satisfied that other adequate measures exist.

Security procedures include:

a. Physically securing information. Any desk or cupboard containing confidential information must be kept locked. Computers should be locked with a password or shut down when left unattended and discretion should be used when viewing personal information on a monitor to ensure that it is not visible to others.
b. Controlling access to premises. Staff should report any person they do not recognise in an entry-controlled area.

Particular care must be taken by Staff who deal with telephone enquiries to avoid inappropriate disclosures. In particular:

a. The identity of any telephone call must be verified before any personal information is disclosed
b. If the caller's identity cannot be verified satisfactorily, then they should be asked to put their enquiry in writing.

c. Do not allow callers to bully you into disclosing information. In case of any problems or uncertainty, contact the Data Protection Officer.

Any personal data we control or process may be held in the following systems and locations, and we are satisfied that there are adequate data protection and data security measures in place:

a. Accounting system –
b. Email system
c. Email marketing service for newsletters
d. Electronic files held – One Drive
e. Paper files on our premises

Copies of personal information, whether on paper or on any physical storage device, must be physically destroyed when they are no longer needed. Paper documents should be shredded and CDs or memory sticks or similar must be rendered permanently unreadable.

4. Personal data breaches

A personal data breach is defined as a security incident that has affected the confidentiality, integrity or availability of personal data. There will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable and this unavailability has a significant negative effect on individuals.

If a personal data breach has occurred, the Charity will take immediate steps to contain it and assess the risk of potential adverse consequences for individuals. If there is a risk to people's rights and freedoms it will be reported to the ICO within 72 hours of becoming aware of the breach. If there is a high risk to those concerned, they will be informed directly and without undue delay. If the breach is unlikely to result in a risk to rights and freedoms, the breach will be investigated, recorded and steps taken to avoid a future recurrence.

5. Staff responsibilities

Staff must ensure that, in carrying out their duties, Cloudy Foundation is able to comply with its obligations under the DPA. In addition, each staff member is responsible for:
a. checking that any personal data that he/she provides to us is accurate and up to date
b. informing us of any changes to information previously provided, e.g. change of address
c. checking any information that we may send out from time to time, giving details of information that is being kept and processed
d. ensuring that if, as part of their responsibilities, they collect information about other people or about other staff, they comply with this policy. This includes ensuring that information is processed in accordance with the DPA, is only processed for the purposes for which it is held, is kept secure, and is not kept any longer than is necessary.
Staff are reminded that the DPA does not just apply to records relating to our staff, but also to any client/customer/donor files/records. Information stored on clients/customers/donors should be reviewed regularly to ensure it is accurate and up to date. All documents, whether

hand written or stored in emails (current or deleted) are potentially disclosable in the event of a request from staff or client/customer/donor.

6. Staff records

We hold personal information about all staff as part of our general staff records. This includes address and contact details, age, date of birth, marital status or civil partnership, educational background, employment application, employment history with GCHC, areas of expertise, details of salary and benefits, bank details, performance appraisals and salary reviews, records relating to holiday, sickness and other leave, working time records and other management records. We may receive and/or retain this information in various forms (whether in writing, electronically, or verbally or otherwise).

This information is used for a variety of administration and management purposes, including payroll administration, benefits administration, facilitating the management of work and staff, performance and salary reviews, complying with record keeping and other legal obligations.

We also process information relating to staff's health, some of which may fall under the definition of 'sensitive personal data'. This includes pre-employment health questionnaires, records of sickness absence and medical certificates (including self-certification of absence forms), night worker assessments, VDU assessments, noise assessments and any other medical reports. This information is used to administer contractual and Statutory Sick Pay, monitor and manage sickness absence and comply with our obligations under health and safety legislation and the Working Time Regulations.

From time to time we may ask staff to review and update the personal information we hold about them. Staff should check this information carefully and inform us of any inaccuracies. However we ask that staff do not wait until asked to update this information, but inform us immediately of any significant change(s).

7. Data security

The need to ensure that data is kept securely means that precautions must be taken against physical loss or damage, and that both access and disclosure must be restricted.

All hard copy personal files are kept in a locked cabinet/room and are not to be removed from the premises. Other information that is stored electronically has appropriate levels of authorisation which prevent unauthorised access.

Only designated responsible personal have access to the personnel records. Line Managers are required not to retain their own copies of personal data, but provide all details to the designated responsible personal, who will ensure the data is filed appropriately.

Data retained on local drives laptops, smartphones and any other electronic equipment that is removed from our offices and such machines must be password protected. Wherever possible all data should be stored on our cloud based system and only accessed by approved employees and volunteers via our permission system.

Staff are responsible for ensuring that any personal data that they hold is stored securely and that personal information is not disclosed either orally or in writing or otherwise to any unauthorised third party.

References that disclose personal information will not be provided to any third party without the data subject's prior authority (unless this is required or permitted by law such as by the police, HMRC, Contributions Agency or similar body.)

Third party processors will be required to provide sufficient guarantees for their data security

measures and compliance with them. A written contract will be in place with each supplier which requires them to dispose of data securely and to provide suitable evidence of this. Checks will be made to ensure that secure data disposal facilities are in place and regular monitoring will take place.
Any staff member who discovers personal or sensitive data in an inappropriate place (for example unknowingly sent to the wrong printer) should immediately pass this to Chief Executive, ensuring that its contents are not revealed to anyone else.

8. Publication of information

Information that is already in the public domain is exempt from the Act. This would include, for example, information contained within externally circulated publications such as brochures and other sales and marketing aids.
Any individual who has good reason for wishing his/her details not to be included in such publications should contact Director of Operations.

9. Subject consent

Our contracts of employment imply the consent of staff to the processing of personal data for the purposes of administration, managing and employing them. This includes: payroll, benefits, medical records, absence records, sick leave/pay information, performance reviews, disciplinary and grievance matters, pension provision, recruitment, family policies (maternity, paternity, adoption etc) and equal opportunity monitoring.
Information about an individual will only be kept for the purpose for which it was originally provided. Staff and managers should not collect data that is simply "nice to have" nor use data for any purpose other than what it was provided for originally.

10. Retention and disposal of data

All staff are responsible for ensuring that information is not kept for longer than necessary. Documents containing any personal information will be disposed of securely, and paper copies will be shredded (not disposed of directly into a normal bin or recycling bin).
Information stored on obsolete electronic equipment (desktops, laptops and other devices) will be erased prior to the equipment being sold, disposed of or reallocated to other staff.

11. Registration

The Data Protection Act 1998 requires every data controller who is processing personal data, to notify and to renew their notification on an annual basis. Failure to do so is a criminal offence.
The Chair of Trustees is our Data Controller and is responsible for ensuring compliance with the Data Protection Act, for notifying and updating the Information Commissioner of our processing of personal data, and for the monitoring and implementation of this policy on behalf of Cloudy Foundation.
Any changes made to the information stored and processed must be brought to the attention of the Chair of Trustees immediately.
Related policies: Social Media (and web-based technology) Policy.

12. Implementation, monitoring and review of this policy

The Chair of Trustees has overall responsibility for implementing and monitoring this policy,

which will be reviewed on a regular basis following its implementation (at least annually) and additionally whenever there are relevant changes in legislation or to our working practices. Any questions or concerns about the interpretation or operation of this policy should be taken up in the first instance with them. Any breach will be taken seriously and may result in formal disciplinary action. Any staff member who considers that the policy has been breached in any way should raise the matter with his/her manager or the Chair of Trustees.

Approval and Review

Approval By	Date	Next Review Date
Trustee Board	Dec 20	Dec 21

Appendix

Personal information we process and what we do with it

Staff

We collect personal information about Staff which:

a. You provide, or we gather, before or during your employment or engagement with us
b. Is provided by third parties, such as references or information from suppliers or another party that we do business with
c. Is in the public domain

The types of personal information that we may collect, store and use about Staff include records relating to:

a. Home address and contact details as well as contact details for your next of kin
b. Recruitment (including your application form or cv, any references received and details of your qualifications)
c. Pay records, national insurance number and details of your taxes and any employment benefits such as pension and health insurance (including details of any claims made)
d. Any sickness absence or medical information provided
e. Telephone, email, internet, fax or instant messenger use
f. Performance and any disciplinary matters, grievances, complaints or concerns in which you are involved.

We will use information to carry out our business, to administer your employment or engagement and to deal with any problems or concerns you may have, including:

a. Sickness records. To maintain a record of your sickness absence and copies of any doctor's notes or other document supplied to us in connection with your health, to inform your colleagues and others that you are absent, as reasonably necessary to manage your absence, to deal with unacceptably high or suspicious sickness absence, to inform reviewers for appraisal purposes of your sickness absence level, to publish internally aggregated, anonymous details of sickness absence levels.
b. Monitoring IT systems. To monitor your use of emails, internet, telephone and fax, computer or other communications or IT resources.
c. Disciplinary, grievance or legal matters. In connection with any disciplinary, grievance, legal, regulatory or compliance matters or proceedings that may involve you.
d. Performance reviews. To carry out performance reviews.

We confirm that the Charity is a Data Controller of the personal information in connection with your employment. This means that we determine the purposes for which, and the manner in which, your personal information is processed.

We will take reasonable steps to ensure that your personal information is kept secure, as described in this policy and in general, we will not disclose your personal information to others outside the Charity. However, we may need to disclose personal information about Staff:

a. For the administration of your employment and associated benefits, e.g. to the providers of our payroll, pension or insurance schemes
b. To comply with our legal obligations or assist in a criminal investigation or to seek legal or professional advice in relation to employment issues, which may involve disclosure to our lawyers, accounts or auditors and to legal and regulatory authorities, such as HM Revenue and Customs
c. To other parties which provide products or services to us.

Beneficiaries

We collect personal information about our beneficiaries which:

a. They or their parents/referrers provide, or we gather, before or during their engagement with us

The types of personal information that we may collect, store and use about our beneficiaries include records relating to:

a. Name
b. Contact information including address, telephone number and email address where appropriate
c. Medical and education information and reason for referral

We will use the information in order to provide you with our charitable services in line with the overall expectation and deliverables of the Charity's project. We will not collect any

personal data from you we do not need in order to provide and administer this service to you.

We may also use your email address to send our newsletters to you, if you have requested us to.

We will take reasonable steps to ensure that your personal information is kept secure, as described in this policy and in general, we will not disclose your personal information to others outside the Charity unless we have your permission or we are required by law to do so.

By providing your personal information to us, you consent to the use of your personal information in accordance with this policy.

Suppliers

We collect personal information about suppliers which:

a. You provide, or we gather, before or during your engagement with us
b. Is provided by third parties, such as information from other suppliers or another party that we do business with
c. Is in the public domain

The types of personal information that we may collect, store and use about suppliers include records relating to:

a. Name and job title
b. Contact information including address, telephone number and email address
c. Bank account details, sort code and account number (if applicable)

We will use information to carry out our business with you/your business such as contacting you to discuss your products and services, place orders with you and pay your invoices. We will not collect any personal data from you we do not need in order to carry out these transactions.

We may also use your email address to send our newsletters to you, if you have requested us to.

We will take reasonable steps to ensure that your personal information is kept secure, as described in this policy and in general, we will not disclose your personal information to others outside the Charity unless we have your permission or we are required by law to do so.

By providing your personal information to us, you consent to the use of your personal information in accordance with this policy.

Other third parties (e.g.schools and colleges, business contacts, networking associates

We collect personal information about other third parties which:

a. You provide, or we gather from you
b. Is provided by third parties, such as information from other parties that we do business with
c. Is in the public domain

The types of personal information that we may collect, store and use about suppliers include records relating to:

a. Name and job title
b. Contact information including address, telephone number and email address

We will use information to carry out business with you/your business such as contacting you to discuss your products and services. We will not collect any personal data from you if we do not need to do so.

We may also use your email address to send our newsletters to you, if you have requested us to.

We will take reasonable steps to ensure that your personal information is kept secure, as described in this policy and in general, we will not disclose your personal information to others outside the Charity unless we have your permission or we are required by law to do so.

By providing your personal information to us, you consent to the use of your personal information in accordance with this policy.