



2nd Chance Project CIC - Data Protection Policy

Scope of Policy

This policy applies to:

- The Henfield Office
- The Netham Sports facility ;
- All sessional workers operating on behalf of 2nd Chance Project CIC at any other location

It applies to paid staff, volunteers and any partnership or freelance organisations.

Policy Operational Date

- 24 May 2011

Policy Review Date

- June 2014
- Company is to review the Data Protection policy every three years.

Purpose of Policy

The purpose of this policy is to enable 2nd Chance Project CIC to:

- comply with the law in respect of the data it holds about individuals;
 - follow good practice;
 - protect 2nd Chance Project's supporters, staff and other individuals
- protect the organisation from the consequences of a breach of its responsibilities.

Brief introduction to Data Protection Act 1998

The Data Protection Act 1998 regulates the collection, storage, use and disclosure of information about individuals by organisations. Any organisation that keeps information about individuals must comply with the act. This article gives a brief introduction to the act and issues related to it.

[The Data Protection Act 1998](#) came into force on 24th October 2001. The Act applies to *personal data* - information about identifiable living individuals that is:

- Held on computer or any other automated system
- Held in a *relevant filing system* (a paper system such as client records system, or a set of files on service users that is organized alphabetically by the name of the person or some other identifier such as case number)
- Intended to go onto computer or into a relevant filing system

The Data Protection Act applies mainly to the Data Controller - the person who decides why and how personal data is processed. This "person" doesn't have to be an individual and in



most cases will be an organization. Individual members of staff or volunteers will merely be agents of the data controller.

The Act has eight Data Protection Principles that cover issues including the processing, accuracy, security and lawfulness of data collection as well as the rights of the Data Subject.

The 8 Principles of the Data Protection Act 1998

The 8 Data Protection Act principles outline the requirements of the legislation, now in force.

Personal data must be:

- Processed fairly and lawfully.
- Processed only for one or more specified and lawful purpose.
- Adequate, relevant and not excessive for those purposes.
- Accurate and kept up to date - data subjects have the right to have inaccurate personal data corrected or destroyed if the personal information is inaccurate to any matter of fact.
- Kept for no longer than is necessary for the purposes it is being processed.
- Processed in line with the rights of individuals - this includes the right to be informed of all the information held about them, to prevent processing of their personal information for marketing purposes, and to compensation if they can prove they have been damaged by a data controller's non-compliance with the Act.
- Secured against accidental loss, destruction or damage and against unauthorised or unlawful processing - this applies to you even if your business uses a third party to process personal information on your behalf.
- Not transferred to countries outside the European Economic Area - the EU plus Norway, Iceland and Liechtenstein - that do not have adequate protection for individuals' personal information, unless a condition from Schedule four of the Act can be met.

Personal Data

This policy applies to information relating to identifiable individuals, even where it is technically outside the scope of the Data Protection Act, by virtue of not meeting the strict definition of 'data' in the Act.

Policy Statement

2nd Chance Project CIC will:

- Comply with both the law and good practice
- Respect individuals' rights
- Be open and honest with individuals whose data is held
- Provide training and support for staff and volunteers who handle personal data, so that they can act confidently and consistently

2nd Chance Project CIC recognises that its first priority under the Data Protection Act is to avoid causing harm to individuals. In the main this means:

- Keeping information securely in the right hands, and
- Holding good quality information.



Secondly, the Act aims to ensure that the legitimate concerns of individuals about the ways in which their data may be used are taken into account. In addition to being open and transparent, 2nd Chance Project CIC will seek to give individuals as much choice as is possible and reasonable over what data is held and how it is used.

Key Risks

2nd Chance Project CIC has identified the following potential key risks, which this policy is designed to address:

- Breach of confidentiality (information being given out inappropriately) — especially at location level.
- Insufficient clarity about the range of uses to which data will be put — leading to Data Subjects being insufficiently informed
- Failure to offer choice about data use when appropriate
- Breach of security by allowing unauthorised access - especially at branch level.
- Failure to establish efficient systems of managing changes to branch volunteers, leading to personal data being not up to date.
- Harm to individuals if personal data is not up to date
- Insufficient clarity about the way sessional workers' or volunteers' personal data is being used e.g. given out to general public.
- Failure to offer choices about use of contact details for staff, volunteers, sessional workers or branch officers

Data Processed by the Project

The 2nd Chance Project holds and processes information about its employees, applicants, students, alumni and other individuals who are defined as “data subjects” under the Data Protection Act. The 2nd Chance Project finds it necessary to process personal data for a variety of reasons from administrating the admissions process and operating payroll, to recording academic process, monitoring attendance and enabling references to be provided

Compliance with Data Protection Act 1998:-

The 2nd Chance project takes the protection of all personal data extremely seriously and is committed to a policy of protecting the rights and freedoms of all individuals in relation to the processing of their personal data in compliance with Data Protection legislation.

The 2nd Chance project has nominated a Data Protection Officer who is responsible for notifying the Information Commissioner, responding to individual requests for access to personal data and framing guidelines and procedures with the aim of ensuring that all personal data processing by the 2nd Chance project complies with the Data Protection Act 1998.



Responsibility of Data Users:-

Staff and students of the 2nd Chance project who are in any way involved with the processing of personal data (see below for definition), are referred to in this policy as “Data Users”. Data Users must ensure that any processing of personal data by them, complies fully with the “2nd Chance project” which include following:

- i) The Data Protection Act 1998
- ii) This Data Protection Policy
- iii) Any additional procedures or guidelines relating to Data Protection matters which may be issued by the 2nd Chanceproject from time to time,

In particular, all Data Users are required to familiarise themselves with the Guidelines and Golden Rules for Compliance contained on the 2nd Chance Project Data Protection policies.

Processing of personal data includes every form of action in relation to that data including: obtaining, recording, holding, using in any way, disclosure, archiving, erasure and destruction.

Whenever a new form of processing personal data is contemplated, those concerned must seek advice to ensure that the proposed processing is lawful and already covered by the 2nd Chance Project notification to the Information Commissioners, which specifies the purposes for which the 2nd Chance Project holds and processes personal data.

Students should only obtain and/or use personal data relating to third parties for approved research or other legitimate 2nd Chance project related purposes, once they have obtained the express consent of an appropriate member of staff who is responsible for their supervision.

All Data Users are warned that, any breach of the Data Protection Act or the 2nd Chance Project Data Protection Rules will be viewed very seriously and may result in legal proceedings being taken against the 2nd Chance Project and disciplinary action being taken against the individuals concerned.

Prohibited Activities

No Data User may at any time, without the prior written authorisation of the Data Protection Officer:

- Adapt a system already in place for processing personal data, to enable it to process data for a different purpose, or in any way use data obtained for one purpose for a supplemental purpose;
- Disclose to any third party outside of the 2nd Chance project personal data relating to an individual without the individual’s express consent.



Personal Data used for Research:-

Before commencing any research which will entail obtaining or using personal data, the researcher (whether a student or a member of staff) and their academic supervisor/Head of Group must give proper consideration to the 2nd Chance Project Data Protection Rules and how these will be properly complied with. In particular, they will need to consider the type of personal data which it is proposed be obtained/ used, the extent to which such data may legitimately be required for the academic objective, how the data will be securely stored and the duration for which it will be retained.

Personal data obtained and/or used for research should be limited to the minimum amount of data which is reasonably required to achieve the desired academic objectives and wherever possible any such personal data should be made anonymous so that the data subjects cannot be identified.

Data Protection Officer

Any queries concerning data protection matters should be raised with the 2nd Chance Project Managing Director/Data Protection Officer who can be contacted by email on james@2ndchanceproject.co.uk.



Confidentiality

Scope

- Information about other organisations, since Data Protection only applies to information about individuals
- Information which is not recorded, either on paper or electronically
- Information held on paper, but in a sufficiently unstructured way that it does not meet the definition of a “relevant filing system” in the Data Protection Act

Understanding of Confidentiality

Normally access will be defined on a “need to know” basis.

No one should have access to information unless it is relevant to their work. This may be relaxed in the case of information which poses a low risk: for example a list of business contacts may be made generally available, even if this means people having access who don't strictly need it.

Where risks can be specifically identified, for example in work with teenagers, discussing how much information will be shared with their parents.

There will always be cases where the organisation feels it is right to break confidentiality, it will be decided on a case-by-case basis whether this is appropriate.

Communication with Data Subjects

2nd Chance Project CIC have a privacy statement for Data Subjects, setting out how their information will be used. This will be available on request, and a version of this statement will also be used on a case-by-case basis whether this is appropriate.

Photographic Records



Photographs taken of students and clients will only be taken by 2nd Chance Project if a consent form has been signed by the subject and if under 18 the written consent of parent or guardian.

Communication with Staff

Staff, volunteers and sessional workers will be required to sign a short statement indicating that they have been made aware of their confidentiality responsibilities. (see Appendix)

Security

Scope

This section of the policy only addresses security issues relating to personal data. It does not cover security of the building, business continuity or any other aspect of security.

Specific Risks

2nd Chance Project has identified the following risks:

- Staff or volunteers with access to personal information could misuse it.
- Sessional workers or, more likely, volunteers could continue to be sent information after they have stopped working for 2nd Chance Project, if their records are not updated promptly.
- Poor web site security might give a means of access to information about individuals once individual details are made accessible on line.
- Staff may be tricked into giving away information, either about supporters or colleagues, especially over the phone, through “social engineering”.

Setting Security Levels

Access to information on the main computer system will be controlled by function and protected by passwords.



Data Recording & Storage

Accuracy

2nd Chance Project is moving towards a single database holding information about all students and clients. Sessional workers may also keep separate information about those they are supporting.

2nd Chance Project will regularly review its procedures for ensuring that its records remain accurate and consistent and, in particular:

- “Substance – Views” ICT systems have been adopted, where possible, to encourage and facilitate the entry of accurate data.
- Data on any individual will be held in as few places as necessary, and all staff and volunteers will be discouraged from establishing unnecessary additional data sets.
- Effective procedures will be in place so that all relevant systems are updated when information about any individual changes.

Staff or volunteers who keep more detailed information about individuals will be given additional guidance on accuracy in record keeping.

Updating

Staff will be updating their systems regarding their students or clients on a weekly / monthly basis. Those data subjects with whom contact ceases are to be archived using the Views system archive facility on a monthly basis.

Storage

- i) Substance is registered with the Information Commissioners Office (ISO number: Z9541305)



ii) Substance holds ISO 27001 Information Security assurance. (There is no higher data security quality assurance).

iii) Data stored in Views is looked after to the highest standards. The system operates via a 2048 bit industry standard Secure Sockets Layer (SSL) which means all data is subject to 128/256 bit encryption. (This is equivalent to online banking security).

iv) Data is stored in a secure data hosting facility in the UK and is backed up 'off site' twice a day

Subject Access

Responsibility

Any subject access requests will be handled by the Data Protection Officer.

Procedure for Making Request

Subject access requests must be in writing. All staff and volunteers are required to pass on anything which might be a subject access request to the Data Protection Officer without delay.

All those making a subject access request will be asked to identify any sessional workers who may also hold information about them, so that this data can be retrieved.

Provision for Verifying Identity

Where the individual making a subject access request is not personally known to the Data Protection Officer their identity will be verified before handing over any information.



Appendix: Confidentiality statement for staff and volunteers

When working for 2nd Chance Project, you will often need to have access to confidential information which may include, for example:

- Personal information about individuals who are supporters or otherwise involved in the activities organised by 2nd Chance Project.
- Information about the internal business of 2nd Chance Project.
- Personal information about colleagues working for 2nd Chance Project.

2nd Chance Project is committed to keeping this information confidential, in order to protect people and 2nd Chance Project itself. 'Confidential' means that all access to information must be on a need to know and properly authorised basis. You must use only the information you have been authorised to use, and for purposes that have been authorised. You should also be aware that under the Data Protection Act, unauthorised access to data about individuals is a criminal offence.

You must assume that information is confidential unless you know that it is intended by 2nd Chance Project to be made public. Passing information between a branch and the UK office, or between 2nd Chance Project and a mailing house, or *vice versa* does not count as making it public, but passing information to another organisation does count.

You must also be particularly careful not to disclose confidential information to unauthorised people or cause a breach of security. In particular you must:



- not compromise or seek to evade security measures (including computer passwords);
- be particularly careful when sending information between the UK office and branches;
- not gossip about confidential information, either with colleagues or people outside 2nd Chance Project;
- not disclose information — especially over the telephone — unless you are sure that you know who you are disclosing it to, and that they are authorised to have it.

If you are in doubt about whether to disclose information or not, do not guess. Withhold the information while you check with an appropriate person whether the disclosure is appropriate.

Your confidentiality obligations continue to apply indefinitely after you have stopped working for 2nd Chance Project.

I have read and understand the above statement. I accept my responsibilities regarding confidentiality.

Signed:

Date: