Exeter Community Initiatives

Policy Name:	**DATA PROTECTION AND INFORMATION SHARING POLICY**
Approved by Council:	**December 2018**
Next Review:	**December 2021**

The Trustees in adopting this policy fully understand their legal obligations and the importance of monitoring and implementing the policy within ECI.

EXETER COMMUNITY INITIATIVES (ECI)
DATA PROTECTION AND INFORMATION SHARING POLICY
(as at 06/12/12 – updated 15/09/16)

1 Introduction

1.1 ECI is a registered charity and company limited by guarantee. Throughout this policy, ECI refers to the organisation as a whole that comprises the work of the individual projects and any support services that are provided corporately.

2 Statement of Intent

2.1 ECI ensures that all data and information held on individuals (**data subjects**) including employees, clients and the public is managed and handled in a sensitive, secure and responsible manner. This includes photographic material. If in doubt about any aspect of this policy, please refer to your line manager for guidance.

2.2 This policy document relates to the Data Protection Act (2018), and the Human Rights Act (1998).

3 Responsibility for the Implementation of this Policy

3.1 The trustees of ECI are ultimately responsible for ensuring that this policy is regularly reviewed and properly implemented.

3.2 The Business Support Manager will be responsible to the trustees for ensuring the overall implementation of this policy.

3.3 Responsibility for implementation within each project will lie with the relevant Project Manager.

3.4 ECI is registered as a **data controller** with the Information Commissioner (Number Z9415436) in relation to 4 purposes: Staff Administration, Administration of Membership Records, Fundraising and Realising the Objectives of a Charitable Organisation or Voluntary Body.

4 Related Policies

4.1 Equalities & Diversity Policy; Criminal And Safeguarding Checks And Employers Duty To Refer Information Policy; Confidentiality Policy.

5 Background

5.1 The Data Protection Act (2018) includes both manual and computerised data and information. It covers all aspects of processing data: collection, holding, access, use, disclosure and destruction.

5.2 Personal data covers both facts and opinions on identifiable, living individuals, which is either being processed or is recorded in a relevant filing system.

5.3 The Human Rights Act 1998 brought the European Convention on Human Rights into UK law and of particular relevance is Article 8. This Article states that everyone has the right to respect for their private and family life, home and correspondence. It is not an absolute right and is qualified by lawful restrictions.

5.4 Personal information about members of staff, volunteers and/or service users will be stored by ECI on commencement of the individual's involvement with ECI.

6 The 7 Data Protection Principles and ECI Policy

6.1 Below is a guide to how ECI has interpreted the 7 principles. **Appendix 1** is a practical Q&A.

Article 5(1) requires that personal data shall be:

"(1) processed lawfully, fairly and in a transparent manner in relation to individuals

- When obtaining personal data from a data subject, staff should ensure that the subject knows why and how the data will be used. See section 8 on Sensitive Data. Consent must be clear and distinguishable from other matters and provided in an intelligible and easily accessible form, using clear and plain language. It must be as easy to withdraw consent as it is to give it.
- The public Data Protection Statement (see **Appendix 3**) is a public summary of our commitment to the principles of the Data Protection Act and should be included or referenced on appropriate publicity material, including the website and verbal conversations.
- Personal data and information collected online will be covered by a privacy statement (see **Appendix 3**)

('lawfulness, fairness and transparency');

(2) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes ('purpose limitation');

(3) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

(4) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes

- See **Appendix 4** for suggested timescales for different types of data
- Information only relevant to the purpose should be collected.
- **Subject Access Requests**: Data subjects can ask to see all information that ECI holds on them, including manual files. The organisation has 1 month to comply with the request and cannot charge for it. See the **Appendix 2** to see how this affects employees.

for which they are processed, are erased or rectified without delay ('accuracy');

(5) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals ('storage limitation');

(6) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')."

- All personal data should be kept securely, either on a password protected database, or if it is in paper format, in a locked filing cabinet.
- Staff using computer systems are only authorised to access data files that are relevant to their area or work.
- Personal data should not be moved or transported. However, there will be times when this is unavoidable and in these circumstances, the employee responsible has a duty of care to ensure the personal data remains as secure as possible.

Article 5(2) adds that:

"The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')."

7 Information Sharing

7.1 As a general principle disclosure of data to third parties, without explicit consent of the data subject, is not allowed and is unlawful.

7.2 There will be some cases in which information regarding employees or clients that will require information to be shared.

7.2.1 Clients & volunteer: information may be shared to benefit or prevent harm to, an individual or for legal purposes – see Appendix 1, specifically A1.10 & A1.11

7.2.2 Employees: information may be shared as in 7.2.1 or to prevent harm to another employee or the organisation – see Appendix 2, specifically A2.1

7.3 If information is to be shared, wherever possible the individual should be fully informed of the consequences of consent or non-consent and the details of the information shared, given to them. Where harm to others may occur (see Child Protection Policy) the individual should not be informed.

8 Sensitive Data

8.1 The Data Protection Act 2018 makes specific provision for sensitive personal data. Sensitive data includes racial or ethnic origin; political opinions; religious or other beliefs; trade union membership; personal health; sex life; criminal proceedings or convictions.

8.2 Sensitive data can only be processed under strict conditions including:

8.2.1 having the explicit consent of the individual data subject;

8.2.2 being required by law to process the data for employment purposes (equal opportunities);

8.2.3 the need to process information in order to protect the vital interests of the data subject or another; and

8.2.4 dealing with the administration of justice or legal proceedings.

8.2.5 Children under 16 but over 13 years old are able to give their own consent. Children under 13 we require parental consent

9 Data Storage

9.1 Information and records relating to service users, staff & volunteers will be stored securely and will only be accessible to authorised staff and volunteers.

9.2 Information will be stored for only as long as it is needed or required to remain in line with statute and will be disposed of appropriately.

9.3 It is ECI's responsibility to ensure all personal and company data is non recoverable from any computer system previously used within the organisation, which has been passed on/sold to a third party.

10 Data Access and Accuracy (Subject Access Requests)

10.1 All Individuals/Service Users have the right to access the information ECI holds about them. ECI will also take reasonable steps to ensure that this information is kept up to date by asking data subjects whether there have been any changes.

This policy, along with any closely related policies, will be updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments made to the Data Protection Act 2018.

Glossary of Terms

Data Controller – The person who (either alone or with others) decides what personal information ECI will hold and how it will be held or used.

Data Protection Act 2018 – The UK legislation that provides a framework for responsible behaviour by those using personal information.

Data Protection Officer – The person(s) responsible for ensuring that ECI follows its data protection policy and complies with the Data Protection Act 2018.

Individual/Service User – The person whose personal information is being held or processed by ECI for example: a client, an employee, or supporter.

Explicit consent – is a freely given, specific and informed agreement by an Individual/Service User in the processing of personal information about her/him. Explicit consent is needed for processing any personal data.

Notification – Notifying the Information Commissioner about the data processing activities of ECI, as certain activities may be exempt from notification.

The link below will take to the ICO website where a self assessment guide will help you to decide if you are exempt from notification:
http://www.ico.gov.uk/for_organisations/data_protection/the_guide/exemptions.aspx

Information Commissioner – The UK Information Commissioner responsible for implementing and overseeing the Data Protection Act 2018.

Processing – means collecting, amending, handling, storing or disclosing personal information.

Personal Information – Information about living individuals that enables them to be identified – e.g. name and address, this also includes email addresses. It does not apply to information about organisations, companies and agencies but applies to named persons, such as individual volunteers or employees within ECI.

Sensitive data – refers to data about:

- Racial or ethnic origin
- Political affiliations
- Religion or similar beliefs
- Trade union membership
- Physical or mental health
- Sexuality
- Criminal record or proceedings

Appendix 1 – Q&A

A1.1 How long should I keep records before destroying them?

This depends on what you are storing. See Appendix 4.

A1.2 When might I want to collect personal data & information?

On a very basic level, you may wish to collect names & contact information for those that attend an activity to ensure you can follow up with further information, or perhaps you wish to make sure they receive a newsletter. Collecting personal data & information may be a pre-requisite of running the activity such as providing training.

More importantly you may wish to collect the information about clients to ensure that you can provide the best service possible and to monitor performance.

A1.3 How do I know what information to collect?

You first need to know exactly how you wish to use the information you collect. Is it to:

- send newsletters?
- monitor the performance of a project?
- monitor equal opportunities?
- report on another organisation's requirements?

On most occasions, the only information you will need from the public will be: Title, Name, Full address, Email, Phone (landline & mobile), Organisation (if applicable) and Website (if applicable). Bank details can also be sought if they are to be a financial supporter. This information is required is to ensure that contact can be made in a variety of ways if required.

When collecting information for performance monitoring this will differ for each situation.

A1.4 What do I do if I want to use photographic material?

When taking photographs always inform those around you that you wish to do so. Give anyone a chance to refuse to be in a photograph and take contact details of anyone that agrees. If children under 18 are present, you must receive consent from a parent or carer. Use the following phrase or similar to below to explicitly receive the persons consent:

"I agree for any photograph of me to be used in any ECI literature or publicity"

When you are clear which photograph you wish to use, out of courtesy, contact those in the photograph and inform them how their photo will be used.

A1.5 Is there a standard phrase I should use on my leaflets or documents when asking for personal data and information?

Yes. ECI wishes to be able to follow up any contact with further publicity about our work: however we need to ensure that individuals actively opt in. Therefore there are two phrases to include:

1 "ECI sends out quarterly newsletters with updates about the work we do. If you want to receive this newsletter please tick the box."

2 "Periodically ECI may wish to send out information regarding our work and the support you can give. If you want to receive this information please tick the box."

A1.6 Where should I store personal data & information?

Personal data and information about staff should be stored in the appropriate electronic or manual filing systems.

Personal data and information about clients should be stored in secure databases and will vary for each project. We currently use secured folders on Office 365.

Personal data and information about other contacts should be stored in the central ECI Shared Contacts.

A1.7 If there is no option and I have to transport some personal data, how should I do this?

Before transporting data, make sure you know what data you are transporting, and a backup copy of the data, in either electronic or hard copy form is left in the office.

Only ECI issued USB data sticks which have been encrypted should be used for the transferral of electronic data. All data sticks will be signed in and out on the USB Register and the individual will have to sign the register to confirm they have had the appropriate training from the IT Administrator.

A1.8 Security

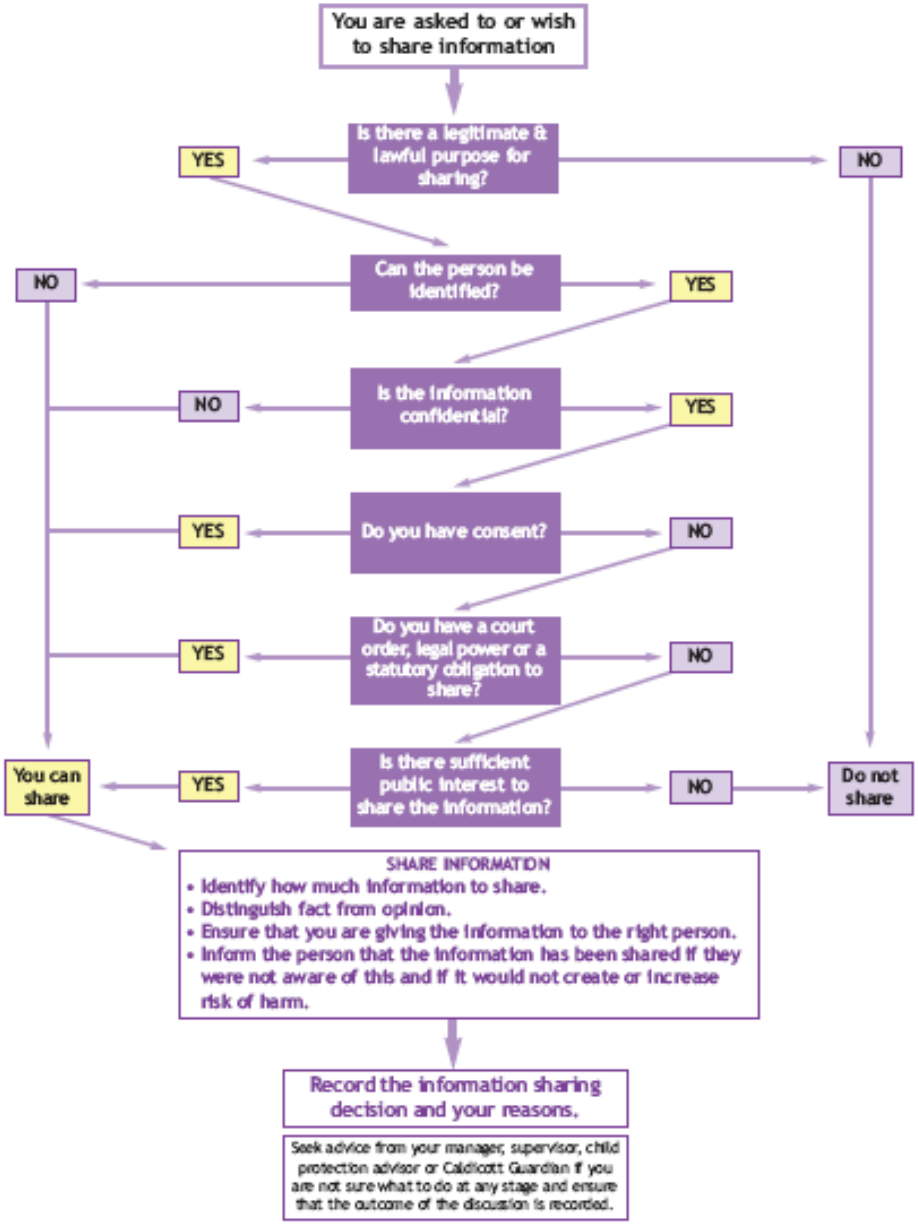
A 3-monthly enforced password change takes place automatically as part of the server setup. Passwords need to be a minimum of 8 characters with a mixture of letters, numbers and symbols. This Kaspersky password security checker can be used as a rough guideline to the strength of a password/passphrase: https://password.kaspersky.com/

If you have to transport manual (paper) files then be very careful about where you place the information, avoiding any situation where you might forget to pick it up.

A1.9 What should I do if I lose personal data?

Inform your manager as soon as possible, who may decide to consult with Chief Executive, and wherever possible retrace your steps and search for the lost data. If after 48 hours you are unable to find the data, you must start contacting the people to which the data relates. If the data is highly sensitive, it should be a manager who contacts the people.

A1.10 How do I know when I can share information?
Please consult with the Chief Executive if there is any question. Follow the flow diagram to decide when to share information when another organisation requests it.



A1.11 How do I decide what is sufficient Public Interest?
The term 'public interest' cannot easily be defined but, in essence it is something which is in the interests of the community as a whole, a group within a community or even an individual. It should be remembered that public interest is not the same as 'interesting to the public'.

There may be circumstances when you want to share personal information with other agencies when you don't have consent to do so from the person whose information you want to share. You are permitted to make a disclosure without a person's consent if you strongly believe that the disclosure is in the best interests of society. For example, if the disclosure would assist in preventing crime and disorder, apprehending or prosecuting offenders, or protecting the health and safety of employees and members of the public or for national defence.

There are also public interests, which in some circumstances may weigh against sharing, e.g. the public interest in maintaining public confidence in the confidentiality of certain services, perhaps in a situation involving a doctor and their patient. Whenever you wish to share information in the 'public interest' you must weigh up the public interest in **disclosing** the information against the public interest in withholding the information.

Appendix 2 – Employee and internal confidentiality

Supervision & appraisals

A2.1 During supervision and appraisal, information discussed will be confidential to the member of staff, his/her supervisor and their line manager, except in the following circumstances:

- There is agreement by both parties to disclose the information outside supervision.
- Behaviour or activities which bring the organisation into disrepute
- Harm to self and others
- Illegal activity (depending on currency and severity)
- Actions of Gross Misconduct
- Activities where Child Protection and Vulnerable Adults Policies apply
- Activities relating to performance or capability
- Activities that may lead to disciplinary action
- The information given by the supervisee will have significant impact on the organisation (e.g. long term sickness)

A2.2 Information disclosed to any member of staff will be confidential to the immediate members of that staff team, unless the conditions of A2.1 apply.

ECI Council, committees and sub-groups

A2.3 The papers of all ECI Council meetings, committees and sub-groups will be available for all ECI staff to look at, unless specifically agreed in advance by the Chair of the relevant Committee. In cases where the Chair of the relevant Committee deems that papers will not be available to staff, they will need to explain the principle of why this decision is being made (e.g. because of individual staffing issues), and the restriction will only apply to papers relating to this particular part of the meeting.

A2.4 Information contained in the papers of all ECI Council meetings, committees and sub-groups should be considered confidential to members of these Committees and ECI staff and will only be disclosed to other parties with the permission of the Chair of the relevant Committee.

Appendix 3 – Data Protection Statement and Privacy Statement

Data Protection Statement

"This is a statement outlining how Exeter Community Initiatives (ECI) meets its obligations under the Data Protection Act 2018 ("the Act"). The statement is subject to regular review to reflect, for example, changes to legislation (Such as GDPR) or to the structure or policies of ECI. The statement is made available to all staff that are expected to apply it.

ECI needs to collect and use certain types of information about people with whom it deals in order to operate. These include: ECI's own employees; supporters, clients, partner organisations, suppliers and others with whom ECI conducts business. In addition to carrying out our own legal functions, ECI may occasionally be required to collect and use certain types of information of this kind to comply with the requirements of other government departments or legislation.

ECI regards the lawful and correct use of personal information as important to the achievement of our objectives, to the success of our operations and to maintaining confidence between those with whom we deal and ourselves. We therefore aim to ensure that our organisation treats personal information lawfully and correctly.

In order to achieve compliance with the Act and its principles, ECI has created and implemented internal policies and procedures, available to all staff, outlining individual and organisational data protection responsibilities and providing detailed guidance on ECI internal data protection procedures.

Personal data and information will only be used for the legitimate purposes for which it was collected. Where any personal data may be disclosed to third parties, consent will be sought prior to disclosure.

Any persons have a right to access the personal data and information that ECI holds and that relates to them. To obtain a copy of such data (or any part of it), in the first instance, please contact ECI. ECI is no longer entitled to make a charge for the provision of such data (or any part of it)."

Privacy Statement

"Exeter Community Initiatives (ECI) receives personal information through this website. You may, for example, be asked for personal information if you want to take advantage of specific services that we offer, such as when registering for updates or requesting copies of our publications. In any case where you provide personal information, we will only use it to deliver the services you have requested."
(This privacy statement only covers ECI's website).

The ECI site does not automatically capture or store personal information, other than logging the user's IP address and session information such as the duration of the visit and the type of browser used. This is recognised by the web server and is only used for system administration and to provide statistics, which ECI uses to evaluate use of the site.

This privacy statement does not cover links within this site to other websites.

The ECI Website complies with the law which changed on 26 May 2011; this law applies to how you use cookies and similar technologies for storing information on a user's equipment such as their computer or mobile device. The website seeks consent for a cookie from the subscriber

or user. The subscriber means the person who pays the bill for the use of the line. The user is the person using the computer or other device to access a website. A Privacy Policy in relation cookies is available on our website: http://www.eci.org.uk/ECIPrivacy-Policy.

Summary of terms

Browser
Used to locate and display web pages via a software application. The most popular ones are Microsoft Internet Explorer, Mozilla Firefox and Google Chrome.

IP (Internet Protocol)
All networks connected to the internet speak IP, the technical standard that allows data to be transmitted between two devices. TCP/IP (Transmission Control Protocol/Internet Protocol) is responsible for making sure messages get from one host to another and that the messages are understood.

IP address
If you are connected to the Internet you have one, for example it may look something like this 123.123.0.1.

Web Server
Delivers (serves up) web pages to your computer.

Cookie
This is a file created by the web browser on the user's PC in response to a message sent from a web server. Each time the web browser subsequently requests a page from the web server, this message is sent back. We only use cookies to record details for systems administration. We do not use cookies to collect or store personal information such as your name or e-mail address.

Appendix 4 – Retention of Personnel and other Related Records Suggested timescales

Background

While the fifth principle of the Data Protection Act states that "**personal data kept for any purpose should not be kept for longer than necessary**", ECI also has to comply with other legal requirements. Data controllers therefore need to have their own retention policy. (www.ico.gov.uk)

This document therefore outlines the period of time for which all personnel and other related records should be held by ECI.

Recruitment		**Responsibility**
Job Application forms and interview notes	6 months after successful appointment for unsuccessful candidates As part of personnel file for successful candidate	Administrator Chief Executive
Diversity and Equality Monitoring forms	6 months after successful appointment for all candidates	Administrator
List of those who have taken application forms	Until successful appointment	Administrator
Staff and Volunteers		
Personnel, and Learning and Development records	6 years after employment ceases	Chief Executive
Trustee Data (Companies House forms)	Permanently for historical purposes	Business Support Manager
DBS	Photocopy of application should be destroyed once DBS confirmation received. The confirmation email should be kept for 6 months	Chief Executive
Accident files	3 years after the date of the last entry	Health and Safety Coordinator
Parental leave records	5 years after birth/adoption of the child or 18 years if the child receives disability allowance	Chief Executive
Redundancy details, calculations of payments, refunds, etc	6 years from the date of redundancy	Chief Executive
Management Team Records	Permanently for historical purposes	Business Support

		Manager
Trustees' Minutes Books	Permanently	Business Support Manager
Disciplinary Hearings and sanctions	All notes and reports will be placed in a sealed envelope in the personnel file. These are then retained for 6 years after employment ceases.	Chief Executive
Records of senior executives	Permanently for historical purposes.	Chief Executive
Time cards	2 years after the annual leave year to which they refer.	Chief Executive
Clients/User Groups		
Client files	6 Months after last contact with client unless specific funders have different requirements	Project Managers
Records relating to children	Until the child reaches age 21	Children's Centre Project Managers
Annual Feedback forms	3 years	Project Managers
Finance		
Income tax and NI returns, income tax records and correspondence with the Inland Revenue	7 years	Finance Manager & Payroll Bureau
Accounting records	7 years	Finance Manager
Maternity pay records	3 years after the end of the tax year in which the maternity period ends	Finance Manager
Sick pay records- calculations, certificates and self certificates	3 years after the end of the financial year to which they relate.	Finance Manager
Wage/salary records	7 years	Finance Manager
Redundancy details, calculations of payments, refunds, notification to the Secretary of State.	12 years from the date of redundancy.	Finance Manager

Shareholders and External Contacts		
Database	If someone ceases to be a **shareholder/supporter/contact** then their file should be removed from the database with immediate effect. Papers relating to the share scheme need to be kept for 7 years as these form part of the accounting records.	Sharescheme Administrator
Policies		
Risk assessments under Health and Safety regulations and other health and safety records	Permanently	Project Managers & Business Support Manager

Sources of Information: http://www.businesslink.gov.uk/bdotg/action/detail?itemId=1074450470&type=RESOURCES

First Adopted	September 2016
1st Review Approved	July 2017
2nd Review Approved	January 2019
3rd Review Approved	
4th Review Approved	
5th Review Approved	
6th Review Approved	
7th Review Approved	