Children in Wales
Plant yng Nghymru

Data Protection Policy

Version & Notes	Submitted to F&HR	Outcome	Submitted to TB	Outcome	Review Date
Version I July 2010					
Version II January 2014	21.2.14	Approved	12.3.14	Approved	April 2015
Version III	16.5.17	Approved	20.6.17	Approved	April 2018

Children in Wales
Plant yng Nghymru

Data Protection Policy

1.0 General Statement

1.1 This policy is designed to ensure that the records of individuals and organisations are handled appropriately by those working for or with Children in Wales.

2.0 Principles

2.1 Children in Wales requires all those affected within the scope of this policy to comply with the Data Protection Act 1998 (the Act). It is the responsibility of individual employees to acquaint themselves with the requirements of the Act. Copies are available from the Administration Manager.

2.2 In the course of your daily work, staff and others may come into contact with and use confidential personal information about people, such as names and addresses or even information about colleagues, young people and their families including health and other private matters. This policy will help ensure compliance with the Act.

2.3 As part of its recognition as a Centre for Accredited Training and as an accredited training provider, Children in Wales, has in place systems and procedures to ensure that the Act is followed correctly by those working with or for Children in Wales.

3.0 Scope of Policy

3.1 This Policy applies to:

- Staff and trustees of Children in Wales
- Assessors/Tutors/Trainers, including Associates of Children in Wales involved in delivering accredited and other training
- Learners, taking part in accredited and other training
- Quality Assurance Managers of awarding bodies

4.0 Related Policies

4.1 This Policy should be read in conjunction with the following:

- Children in Wales Accredited Training Policy Series
- Children in Wales Staff induction and training procedure

- Safeguarding Policy
- IT Policy
- Social Media Policy

5.0 Guidance

5.1 Appendix 1 sets out guidance for staff including:

- The principles which should be followed when making decisions about data protection
- The data protection procedures that should be followed

5.2 If there is any doubt about the disclosure of personal information, seek advice from a line manager or, if he/she is not available speak to, a member of the Corporate Management Team. If this is not possible, then do not disclose the information concerned.

5.3 There may be project specific guidance added to this Policy from time to time.

6.0 Appendices

6.1 Appendix 1: Guidance, Principles & Procedures to be followed in relation to Data Protection

Appendix 1

Guidance, Principles & Procedures to be followed in relation to Data Protection

1. Introduction

1.1 Children in Wales requires all staff to comply with the Data Protection Act 1998 (the Act). It is the responsibility of individual employees to acquaint themselves with the requirements of the Act. Copies are available from the Administration Manager.

1.2 In the course of your work, you may come into contact with and use confidential personal information about people, such as names and addresses or even information about colleagues, young people and their families including health and other private matters. This policy will help you ensure that you do not breach the Act, which provides strict rules in this area.

1.3 If you are in any doubt about what you may or may not do, seek advice from your line manager or if he/she is not available speak to one of the Corporate Management Team. If you cannot get in touch with either, then do not disclose the information concerned.

2. Types of personal data

2.1 The types of personal data that Children in Wales may be required to handle include information about current, past and prospective employees, Trustees, associates, volunteers, casual workers, young people, learners, members or other service users of Children in Wales.

2.2 The personal data, which may be held on paper or on a computer or other media, is subject to certain legal safeguards specified in the Act and other regulations. The Act imposes restrictions on how Children in Wales may process personal data, and a breach of the Act could give rise to criminal sanctions as well as bad publicity for the organisation.

3. Purpose of the Policy

3.2 The purpose of this policy is to enable Children in Wales to:

a. comply with the law in respect of the data it holds about individuals;
b. follow good practice;
c. protect Children in Wales' members, staff and other individuals, and
d. protect the organisation from the consequences of a breach of its responsibilities.

3.3 Children in Wales will:

a. comply with both the law and good practice;
b. respect individuals' rights;
c. be open and honest with individuals whose data is held, and

d. provide training and support for staff and volunteers who handle personal data, so that they can act confidently and consistently.

4. Scope of the Policy

4.1 This policy sets out Children in Wales's rules on data protection and the eight data protection principles contained in the Act. These principles specify the legal conditions that must be satisfied in relation to the obtaining, handling, processing, transportation and storage of personal data.

4.2. Children in Wales's Data Protection Compliance Officer is responsible for ensuring compliance with the Act and with this policy**.** The Data Protection Compliance Officer is the Administration Manager. Any questions or concerns about the interpretation or operation of this policy should be taken up with the Data Protection Compliance Officer.

4.3 This policy is not part of the contract of employment that employees are issued when they join Children in Wales, and Children in Wales may amend it at any time. However, it is a condition of employment that employees and others who obtain, handle, process, transport and store personal data will adhere to the rules of the policy. Any breach of the policy will be treated as gross misconduct and may be a criminal offence.

4.4 Any employee who considers that the policy has not been followed in respect of personal data about themselves or others should raise the matter with their line manager and with Children in Wales's Data Protection Compliance Officer in the first instance.

4.5 Each project or department where personal data is handled is responsible for drawing up its own operational procedures (including induction and training), to ensure that good data protection practice is established and followed.

5. Definition of Data Protection Terms

5.1 'Data' - is recorded information whether stored electronically, on a computer, or in certain paper-based filing systems.

5.2 **'**Data subjects' - for the purpose of this policy 'data subjects' include all living individuals about whom Children in Wales holds personal data. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal information.

5.3 'Personal data' **-** means data relating to a living individual who can be identified from that data (or from that data and other information in possession of Children in Wales). Personal data can be factual (such as a name, address or date of birth) or it can be an opinion (such as a performance appraisal). It can even include a simple e-mail address. It is important that the information has the data subject as its focus and affects the individual's privacy in some way. Mere mention of someone's name in a document does not constitute personal data,

but personal details such as someone's contact details or salary would still fall within the scope of the Act.

5.4 'Data controllers' **-** these are the people or organisations who determine the purposes for which, and the manner in which, any personal data is processed. They have a responsibility to establish practices and policies in line with the Act. Children in Wales is the data controller of all personal data used in its business.

5.5 'Data users' - these include employees, Trustees, casual workers and volunteers whose work involves using personal data. Data users have a duty to protect the information they handle by following Children in Wales's data protection and security policies at all times.

5.6 'Data processors' - include any person who processes personal data on behalf of a data controller. This could include other organisations which handle personal data on Children in Wales's behalf.

5.7 'Processing' - this refers to any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.

5.8 'Sensitive personal data' - includes information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition or sexual life, or about the commission of, or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in such proceedings. Sensitive personal data can only be processed under strict conditions, including a condition requiring the express permission of the person concerned.

5.9 'Data Access Request' – refers to a request received from a data subject to view, amend, delete or destroy data held by the data controller.

6. Data Protection Principles

6.1 Anyone processing personal data must comply with the eight enforceable principles of good practice that are set out in the Data Protection Act 1998. These are:

Transparency and choice

1. Data must be processed fairly and lawfully
2. Data should only be obtained and processed for one or more specified purposes

Good quality data

3. Data must be adequate, relevant & not excessive in relation to the purpose(s) for which it is processed
4. Data must be accurate and where necessary up to date
5. Data processed for any purpose(s) must not be held longer than is necessary for that purpose

Looking after people

6. Data must be processed in line with the rights of Data Subjects
7. Appropriate measures must be taken against unauthorised or unlawful processing of data, and accidental loss or damage
8. Data should not be transferred to a country / territory outside the EEA (European Economic Area) unless there is an adequate level of protection in place for the processing of personal data

More detail is provided on these principles below.

6.2 If you work in the HR department, you must refer to the organisation's further detailed information on the handling and storage of personal data. If you work in one of Children in Wales's projects, you must also follow the rules applicable to the type of work carried out on that project.

6.3 Data must be processed fairly and lawfully

6.3.1 The Act is intended not to prevent the processing of personal data, but to ensure that it is done fairly and in a way that does not adversely affect the rights of the data subject. The data subject must be told who the data controller is (in this case Children in Wales), who the data controller's representative is (in this case the Data Protection Compliance Officer), the purpose for which the data is to be processed by Children in Wales, and the identities of anyone to whom the data may be disclosed or transferred.

6.3.2 For personal data to be processed lawfully, certain specific conditions have to be met. These include, among other things, a requirement that the data subject has consented to the processing (but consent can be implied in certain limited circumstances), or that the processing is necessary for the legitimate interest of the data controller or the party to whom the data is disclosed. When sensitive personal data is being processed, additional conditions must be met. In most cases the data subject's explicit consent to the processing of such data will be required.

6.4 Data should only be obtained and processed for one or more specified purposes

6.4.1 Personal data may only be processed for the specific purposes notified to the data subject when the data was first collected, or for any other purposes specifically permitted by the Act. This means that personal data must 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 must be informed of the new purpose before any processing occurs.

6.5 **Data must be adequate, relevant & not excessive in relation to the purpose(s) for which it is processed**

6.5.1 Personal data should only be collected to the extent that it is required for the specific purpose notified to the data subject. Any data which is not necessary for that purpose should not be collected in the first place.

6.6 Data must be accurate and where necessary up to date

6.6.1 Personal data must be accurate and kept up to date. Information which is incorrect or misleading is not accurate; therefore steps should 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 should be destroyed.

6.6.2 Children in Wales will regularly review its procedures for ensuring that its records remain accurate and consistent and, in particular:

a. Information and Communication Technology systems will be designed, where possible, to encourage and facilitate the entry of accurate data.
b. Data on any individual will be held in as few places as necessary, and the establishment of unnecessary additional data sets will be discouraged.
c. Effective procedures will be in place so that all relevant systems are updated when information about any individual changes.
d. Staff or volunteers who keep more detailed information about individuals will be given additional guidance on accuracy in record keeping.

6.7 Data processed for any purpose(s) must not be held longer than is necessary for that purpose

6.7.1 Personal data should not be kept longer than is necessary for the purpose. This means that data should be destroyed or erased from Children in Wales's systems when it is no longer required.

6.8 Data must be processed in line with the rights of Data Subjects

6.8.1 Data must be processed in line with data subjects' rights. Children in Wales is committed to ensuring, wherever possible, that data subjects are aware:

a. that their data is being processed;
b. for what purpose it is being processed;
c. what types of disclosure are likely; and
d. how to exercise their rights in relation to the data.

6.8.2 Data subjects will generally be informed in the following ways:

a. Employees: in the staff handbook
b. Volunteers and Casual Workers: in the relevant support information pack

c. Trustees: during induction
d. Supporters and service users: when they sign up (on paper, on line or by phone)

6.8.3 Information about Children in Wales' supporters and service users will only be made public with their consent (this includes photographs.)

6.8.4 Children in Wales may receive information from an external organisation which contains personal information about members of that organisation who are not members or supporters of Children in Wales. For example, grant applicant/recipient organisations may supply Children in Wales with personal information on beneficiaries of organisations, perhaps in case studies or reports. Children in Wales will only process such data where the organisation supplying this information confirms in writing that the data subject has consented to the use and storage of that information by Children in Wales.

6.9 Data subjects have a right to:

a. Request access to any data held about them by a data controller (a data access request);
b. Prevent the processing of their data for direct-marketing purposes;
c. Ask to have inaccurate data amended; and
d. Prevent processing that is likely to cause damage or distress to themselves or anyone else.

6.10 **Collecting data from children and parental consent**

6.10.1 In UK, there is no set age for a 'child' when gathering data but it is important to assess *understanding* as well as age when collecting and using data about a child fairly. However, parental consent is usually required to collect data from children under age of 12, *and* from those over 12 where there is a greater risk. Appropriate explanatory language should be used.

6.10.2 It is good practice to seek parental consent if collection / use of information about a child is likely to result in:

a. Disclosure of a child's name and address to a third party
b. The use of a child's contact details for marketing purposes
c. The publication of a child's image on a website that anyone can see
d. Making a child's contact details publicly available
e. The collection of personal data about third parties

6.11 Appropriate measures must be taken against unauthorised or unlawful processing of data, and accidental loss or damage

6.11.1 In relation to emails and faxes, you should follow the guidance in the organisation's internet and email policy, as well as the guidance set out in this policy.

6.11.2 Pay particular attention to the risks of transmitting confidential employee information by email or fax:

a. Transmit information between locations only if a secure network or comparable arrangements are in place or if, in the case of email, encryption is used.
b. Ensure that all copies of email and fax messages received by managers are held securely.
c. The organisation provides a means by which managers can effectively expunge emails that they receive or send from the system and you are responsible for doing so.
d. The organisation draws your attention to the risks of sending confidential, personal information by email or fax.
e. Ensure that the information systems' security policy properly addresses the risk of transmitting employee information by email.

6.12 **Data should not be transferred to a country / territory outside the EEA (European Economic Area) unless there is an adequate level of protection in place for the processing of personal data**

6.12.1 Do not transfer employee data to countries outside the European Economic Area (EEA) unless:

a. the destination country has been designated as providing adequate protection by the European Commission;
b. the destination country is the US and the recipient has signed up to the "safe harbour" principles;
c. the employee whose data is concerned has been told about the intended transfer and has agreed to it;
d. the transfer is to an organisation that acts only as a processor, the processor is reliable, the country in which it is located is stable and the required controller-processor contract is in place; or
e. steps have been taken to ensure that, taking account of all the circumstances of the transfer and the Information Commissioner's guidance on international transfers, adequate protection is provided in other ways.

6.12.2 If you propose to export any personal data from the EEA/UK to another country, the organisation will normally require the recipient to sign in advance the standard contractual clauses of the European Commission. Please contact the Data Protection Compliance Officer for further information.

7. TUPE

7.1 Children in Wales will transfer personal data to new employers in situations involving the transfer of staff from the organisation as defined by the Transfer of Undertakings (Protection of Employment) Regulations 2006 (TUPE). This information will be disclosed to new employers following the ratification of the transfer agreement by Children in Wales and all relevant parties.

8. Data Security

8.1 Children in Wales must ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data. Data subjects may apply to the courts for compensation if they have suffered damage from such a loss.

8.2 The Act requires Children in Wales 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. Personal data may only be transferred to a third-party data processor if it agrees to comply with those procedures and policies, or if it puts in place adequate measures itself.

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

a. 'Confidentiality' means that only people who are authorised to use the data can access it.
b. 'Integrity' means that personal data should be accurate and suitable for the purpose for which it is processed.
c. 'Availability' means that authorised users should be able to access the data if they need it for authorised purposes.

8.4 Security procedures include:

a. Entry controls: Any stranger seen in entry-controlled areas should be reported.
b. 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).
c. Methods of storage: Archived paper records containing confidential information are stored securely on or off site.
d. Methods of disposal: Paper documents should be shredded. CD-ROMs and DVDs should be physically destroyed when they are no longer required.
e. Equipment: Data users should ensure that individual monitors do not show confidential information to passers-by and that they log off (manually or automatically) from their PC when it is left unattended for any period.
f. Passwords and Encryption: Passwords/encryption/software packages are used to safeguard databases and removable media.

9. Retention of Records

9.1 In relation to the retention of records, the organisation follows the retention guidelines recommended by the Information Commissioner in its Employment Practices Code.

9.2 There is a statutory requirement for the retention of certain records listed in the table below. Recommended retention periods for other employment records are also indicated below, however Children in Wales or its projects may require a longer or different retention period.

Statutory Retention Periods	
Annual leave records	2 years after the year in which they were made
Maternity leave records	3 years after the end of the tax year in which the leave period ends
Payroll and tax information	6 years
Accident Register	3 years from end of last entry (or where the accident relates to a child or young adult when that person reaches the age of 21)

Recommended retention periods	
Recruitment records	One year
Employment records, including sickness records	6 years from end of employment, except for Senior Managers whose records should be kept permanently
References given on behalf of employees	6 years from reference/end of employment
Parental leave/unpaid leave/special leave	5 years

10. Confidentiality

10.1 Children in Wales recognises that confidentiality applies to a much wider range of information than data protection.

10.2 Where anyone within Children in Wales feels that it would be appropriate to disclose information in a way contrary to this Policy, or where an official disclosure request or subject access request is received, this will only be done with the authorisation of the Data Protection Compliance Officer. All such disclosures will be documented.

11. Dealing with Data Subject Access Requests

11.1 A formal request from a data subject for information that Children in Wales holds about them must be made in writing, unless the data subject has a disability or other reason within the scope of the Equality Act (2010) which prevents them from doing so. Employees who receive a written request should forward it to the Data Protection Compliance Officer (CIW Administration Manager) immediately. Such a request must be answered within the statutory period, currently 40 days.

11.1.1 Steps should be taken to ensure the identity of the person making the request for information before sensitive data is released.

11.1.2 Data should not be altered between the time of the request and the release of the information, unless changes are routine.

11.2 When receiving telephone enquiries, employees should be careful about disclosing any personal information held on Children in Wales's systems. In particular they should:

a. Check the caller's identity to make sure that information is only given to a person who is entitled to it;
b. Suggest that the caller put their request in writing where the employee is not sure about the caller's identity and where their identity cannot be checked;
c. Refer to their line manager or the Data Protection Compliance Officer for assistance in difficult situations. Employees should not feel pressured into disclosing personal information.

12. Direct Marketing

12.1 Children in Wales will treat the following unsolicited direct communication with individuals as marketing:

a. seeking donations and other financial support;
b. promoting any Children in Wales services;
c. promoting Children in Wales events;
d. promoting sponsored events and other fundraising exercises

12.2 Whenever data is first collected which might be used for any marketing purpose, this purpose will be made clear and the data subject will be given a clear opt out.

12.3 Whenever e-mail addresses are collected, any future use for marketing will be identified and the provision of the address made optional.

13. Staff Training and Responsibilities

13.1 Information for employees is contained in the staff handbook.

13.2 All staff that have access to any kind of personal data will have their responsibilities and this policy outlined during their induction procedures.

13.3 Children in Wales will provide opportunities for staff to explore data protection issues through training, team meetings, and supervisions.

13.4 Consent will normally not be sought for the processing of most information about employees, casual Workers and volunteers, with the following exceptions:

a. employee details will only be disclosed for purposes unrelated to their work for Children in Wales (e.g. financial references) with their consent; and
b. casual workers will be given the choice over which contact details are to be made public.

13.5 Information about volunteers and Trustees will be made public according to their role, and consent will be sought for :

a. the means of contact they prefer to be made public,
b. any publication of information which is not essential for their role.

14. Using Children in Wales' Main Database

14.1 Children in Wales uses a computerised database to keep records of various individuals and organisations. These individuals can be: members; non-members; voluntary sector workers; local and national government departments; professionals such as solicitors; paediatricians and others.

14.2 The database may be used for mailing these individuals and organisations about, but not exclusively:

a. Conferences/Events
b. Publications
c. Consultations
d. Research

14.3 In order for Children in Wales to keep these records on a database it is necessary to comply with the Data Protection Act 1998. To do this the following must be ensured:

a. It may be necessary for Children in Wales to register with the office of the Data Protection Commissioner. This should be verified annually.
b. Staff will be made aware of this Data Protection Policy and ensure that they comply with it at all times.
c. Membership, conference and other booking forms must include a Data Protection Statement that allows the individual the opportunity to:
    i. Opt out of being put on the database
    ii. Request that Children in Wales does not pass their details on to any other organisation
d. Any individual who requests to opt out of being put on the database will be removed from it. If an individual requests that their information is not passed onto any other organisation this will be indicated on the database.
e. Any individuals who are mailed and who have not previously received a Data Protection Statement from Children in Wales must be sent one. This must give them the opportunity to opt out of being on the database, or not having their details passed to other organisations as above.
f. Staff must ensure that they never pass on information about any individual who has requested that their details are not passed on.

15. Policy Review

15.1 This policy will be reviewed annually.