DATA PROTECTION POLICY

Community Learning Partnerships regards the lawful and correct processing of personal and sensitive data as an integral part of its purpose and vital for maintaining confidence between employees, volunteers, service users and other stakeholders whom we process data about, on behalf of, and for ourselves.

General Data Protection Regulations (GDPR) and The Data Protection Act 2018 (DPA) contains principles affecting an individual's personal records. The purpose of this policy is to provide guidance about the protection, sharing and disclosure of employee, volunteer and service user data, but it is important to stress that maintaining confidentiality and adhering to data protection legislation applies to anyone handling personal data or sensitive data on behalf of Community Learning Partnerships.

This policy is also in place to ensure that no breach of these requirements occurs. If you are in any doubt what information you can or cannot disclose and to whom, do not disclose the personal information until you have sought further advice from a member of the Leadership Team.

You should be aware you and/or Community Learning Partnerships can be criminally liable if you knowingly or recklessly disclose personal data in breach of this policy. A serious breach of data protection will result in disciplinary action in line with internal procedures. Where information is accessed without authority, this constitutes as gross misconduct and could lead to dismissal.

1. Information Commissioner

The DPA requires certain data controllers (e.g. organisations) to register with the Information Commissioner Officer (ICO) the categories of data they hold about people and what they do with it.

Community Learning Partnerships are registered with the ICO. Data Protection Registration Number: Z1046101.

2. Definitions of Personal Data and Sensitive Personal Data

- All identifiable data of an individual
- All identifiable employee data
- All identifiable service user/client data
- All other personal data processed by Community Learning Partnerships

Examples of personal identifiable data Community Learning Partnerships' processes include:

- Names, addresses, emails, phone numbers and other contact information
- Financial information
- National insurance numbers and payroll data
- Health information
- Service user/client data
- Photographs
- DBS (criminal record checks)

Certain types of data are regarded as sensitive and attract additional legal protection. Sensitive personal data is considered to be any data that could identify a person such as:

- Racial or ethnic origin of the data subject
- Political opinions
- Religious beliefs or other beliefs of a similar nature
- Membership of a trade union
- Physical or mental health condition
- Sexual life
- Commission or alleged commission of any offence
- Details of bank account, national insurance number, any ID details such as passport/driving licence etc.

3. Data Protection Principles

There are eight data protection principles that are central to the DPA. Community Learning Partnerships and all of its employees must comply with these principles at all times in its information handling practices. The eight principles are:

- **Principle 1**: personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless specific conditions are met. See The Conditions of Processing guidance. What are the conditions for processing? | ICO
- **Principle 2**: personal data shall be obtained only for one of more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose of those purposes.
- **Principle 3:** personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
- **Principle 4:** personal data shall be accurate and up to date
- **Principle 5:** personal data processed for any purpose or purposes shall be kept for no longer than necessary.
- **Principle 6:** personal data shall be processed in accordance with the right of data subjects under this Act.
- **Principle 7:** appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data
- **Principle 8:** personal data shall not be transferred to a country or territory outside the European Economic Area (EEA).

Consent to personal information being held
The organisation holds personal data about you and by signing your contract of employment, volunteer agreement or course registration form you have consented to that data being processed by us. Agreeing to the processing of your personal data is a condition of your employment or participation with Community Learning Partnerships. Community Learning Partnerships will also hold limited sensitive information about its employees, volunteers or service users for example, sickness and absence records and health information.

Personal information on learners is also held for course and funding purposes. Learners will be made fully aware of the reasons for the information and how it will be held and used.

Personal data and sensitive personal data must not be used other than for the specific purposes required to deliver a product or service

All data collected from young people under the age of 16, unless there are concerns about mental capacity, in which case this should be extended, is to be treated as sensitive personal data.

A record can be computerised and/or in manual form. It may include such documentation as;

- Manually stored paper data e.g. employee or learner records
- Hand written notes
- Letters to and from Community Learning Partnerships
- Electronic records

Back up data (i.e. Archived data or disaster recovery records) also falls under the DPA, however a search within them should only be conducted if specifically asked for by the data subject.

4. The right to access personal information
The DPA gives every living person (or authorised representative) the right to apply for access to the personal data which organisations (data controllers) hold about them irrespective of when and how they are compiled i.e. written records, electronic and manual records held in a secure file, subject to certain exemptions. This is called a Subject Access Request. The DPA treats personal data relating to employees, volunteers and service users alike. Individuals also have the right to request that any inaccurate data be corrected or removed.

5. Practical implications
Understanding and complying with the principles is the key to understanding and complying with our responsibilities as a data controller. Therefore, Community Learning Partnerships will, through appropriate management and strict application of criteria and controls:

- Ensure that there is a lawful ground for using the personal data.
- Ensure that the use of the data is fair and that it will meet one of the specified conditions.
- Only use sensitive personal data where Community Learning Partnerships has obtained the individual's explicit consent, unless an exemption applies.
- Only use sensitive personal data, if it is absolutely necessary for Community Learning Partnerships to use it.

- Explain to individuals, at the time their personal data is collected, how that information will be used.
- Only obtain and use personal data for those purposes which are known to the individual.
- Personal data should only be used for the purpose it was given. If we need to use the data for other purposes, further consent may be needed.
- Only keep personal data that is relevant to Community Learning Partnerships.
- Keep personal data accurate and up to date.
- Only keep personal data for as long as is necessary.
- Always adhere to Subject Access Requests and be receptive to any queries, requests or complaints made by individuals in connection with their personal data.
- Always allow individuals to opt-out of receiving bulk information. Community Learning Partnerships will always suppress the details of individuals who have opted out of receiving information (e.g. marketing).
- Will always give an option to "opt in" when consent is needed to share personal data unless there is a statutory/ legal reason to do so.
- Take appropriate technical and organisational security measures to safeguard personal data.

In addition, Community Learning Partnerships will ensure that:

- Everyone managing and handling personal data and sensitive personal data understands that they are legally responsible for following good data protection practice and has received and read the data protection policy.
- Everyone managing and handling personal data and sensitive personal data is appropriately supervised by their line manager.
- Enquiries about handling personal data and sensitive personal data is appropriately supervised by their line manager.
- Enquiries about handling personal data and sensitive personal data are promptly and courteously dealt with.
- Methods of handling personal data and sensitive personal data are regularly assessed and evaluated by the Leadership Team.
- A review and audit of data protection arrangements is undertaken annually.
- Methods of handling personal data and sensitive personal data are regularly assessed and evaluated by the Leadership Team.
- Performance with personal data and sensitive personal data handling is regularly assessed and evaluated by the Leadership Team.
- Formal written Data Sharing Agreements are in place before any personal data and sensitive personal data is transferred to a third party.

6. Roles and Responsibilities

Maintaining confidentiality and adhering to GDPR and data protection legislation applies to everyone at Community Learning Partnerships. Community Learning Partnerships will take necessary steps to ensure that everyone managing and processing personal data understands that they are responsible for following good data protection practice. Employees will receive a copy of the policy at their induction and also receive relevant updates and training as required.

All Employees and volunteers have a responsibility to:

- Observe all guidance and codes of conduct in relation to obtaining, using and disclosing personal data and sensitive personal data.
- Obtain and processing personal data and sensitive personal data only for specified purposes.
- Only access personal data and sensitive personal data that is specifically required to carry out their activity or work.
- Record data correctly in both manual and electronic records.
- Ensure any personal data and sensitive personal data held is kept secure.
- Ensure that personal data and sensitive personal data is not disclosed in any form to any unauthorised third party.
- Ensure personal data and sensitive personal data is sent securely; and
- Read and understand the policy, raising any questions to check understanding.
- Failure to adhere to any guidance in this policy could mean an individual(s) being criminally liable for deliberate unlawful disclosure under the DPA. This may result in criminal prosecution and/or disciplinary action.

All Managers are responsible for:

- Determining if their programme holds personal data and sensitive personal data and ensuring that the data is adequately secure, access is controlled, and that the data is only used for the intended purposes(s);
- Provide clear messaging to those in their teams about data protection requirements and measures.
- Ensure personal and sensitive personal data is only held for the purpose intended.
- Ensure personal and sensitive personal data is not communicated or shared for non-authorised purposes; and
- Ensure personal and sensitive personal data is encrypted when transmitted or appropriate security measures are taken to protect when in transit or storage.

Data Protection Officer/Leadership Team members' responsibilities include:

- Ensuring compliance with legislation principles.
- Ensure employees and volunteers receive a copy of relevant policies and understand their responsibilities and receive training as necessary.
- Ensuring notification of processing of personal data and sensitive personal data to the Information Commissioner is up to date.
- Providing guidance and advice to employees in relation to compliance with legislative requirements.
- Auditing data protection arrangements annually.
- Reporting on any breaches of Data Protection legislation.
- Reviewing the document retention schedule to ensure documents are destroyed and kept for no longer than is necessary.

Leadership team members have overall responsibility for data protection within Community Learning Partnerships and to ensure compliance to DPA and GDPR.

The Information Commissioner Office (ICO) is responsible for overseeing compliance e.g. investigating complaints, issuing codes of practice and guidance, maintaining a register of data protection officers. Any failure to comply with DPA may lead to investigation by the ICO which could result in serious financial or other consequences for Community Learning Partnerships.

7. Data Protection whilst working from home

Whether you regularly work remotely or only occasionally, it remains of the utmost importance that data protection is considered and that the handling and storing of personal information securely is maintained at all times to prevent data breaches from happening. All staff have a legal responsibility to ensure that this policy is complied with at all times wherever they are working.

All employees, whilst working remotely, take responsibility to follow the measures that are in place to ensure the organisation remains legally compliant. Employees must follow the storage and data protection procedures as detailed within this policy. Electronic documents must be saved to the network drives and not to the hard drive of laptops.

All laptops have firewalls and anti-virus software, employees must ensure that when they are prompted, that the latest version of this software is updated. This prevents unauthorised access to devices or network.

All laptops are password protected, and each employee has a user profile and log-in. When logging in remotely Office 365 will ask for a two-factor authentication code which will be sent to a mobile number, or alternative email address.

Hard copies of documentation must not be left lying around, you should ensure that documents are stored in a place where there is a low possibility or other people accessing them and preferably in a locked drawer.

8. Data received on mobile devices

Where documentation cannot be collected in hard or electronic copies via email, then a temporary arrangement has been applied where documents can be received by taking photographs and sending via WhatsApp. This method should only be used where no alternative option is available and where participants consent to send copies by this method. Any documents/images received must be deleted as soon as possible, ideally the same day. Any back-up copy must also be deleted.

9. Breach of Policy

In the event that an employee fails to comply with this policy, the matter may be considered as misconduct and dealt with in accordance with Community Learning Partnerships' Disciplinary Policy and procedure.

Dealing with a Data Breach

If a data breach is suspected, the person who identified the breach should immediately:

- Notify the relevant department manager and
- Notify the Data Protection Officer/Leadership Team member

Following notification of a breach, the Data Protection Officer will take the following actions as a matter of urgency:

Assess the risks associated with the breach.
Inform the appropriate people and organisations that the breach has occurred.
Notify the service user/employee/volunteer if data has been breached.
Review our response and update our information security

APPENDIX 1

Data Subject
Means an individual who is the subject of personal data or sensitive personal data. This includes an employee, volunteer, service user or other identifiable individual.

Data Controller
A controller determines the purposes and means of processing personal data.

The data controller is Community Learning Partnerships for employee/volunteer/service user data.

Data Processor
A processor is responsible for processing personal data on behalf of a controller.

Third Party
In relation to personal data or sensitive personal data, third party means any person other than the data subject, the data controller, or any data processor or other person authorised to process data for data controller or processor. For example, the police or HMRC.

Processing
Means recording or holding data or carrying out any operations on that data; including organising, altering or adapting it; disclosing the data or aligning, combining, blocking or erasing it. Essentially if you have it, you are processing it.

Data Breach
Is a failure leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data or sensitive personal data.

Subject Access Request
This is a written, signed request (which includes emails and other written formats) from an individual to see data held on them. The Data Controller must provide all such information in a readable form within 40 days of receipt of the request.

Created by: Lisa Metcalf	Date: 06/03/2008
Reviewed by: Jon Hosegood – Trustee, Jenny Harris – Senior Manager	Date 04/10/2024
Amended by: Amended by Jenny Harris	Date: 04/10/2024
Approved by: Jon Hosegood	Date: 04/10/2024
Version: 8	