

DATA PROTECTION POLICY

1. Introduction

- 1.1 UK data protection law ensures a balance between an individual's right to privacy and the lawful processing of personal data undertaken by organisations. It aims to protect the rights of individuals about whom data is obtained, stored, processed or supplied that requires that organisations take appropriate security measures against unauthorised access, alteration, disclosure or destruction of personal data.
- 1.2 Community Links Training & Enterprise (Community Links) needs to gather and use certain information about individuals. These can include customers, learners, suppliers, business contacts, employees and other people the organisation has a relationship with or may need to contact. This policy describes how we handle personal data and this policy applies to all personal data, regardless of whether it is in paper, electronic or verbal format.
- 1.3 This policy ensures Community Links:
 - Complies with current data protection laws and follows good practice
 - Protects the rights of staff, customers and partners
 - Is open about how it stores and processes individuals' data
 - Protects itself from the risk of a data breach

2. Scope

- 3.1 This policy applies to all staff employed by Community Links and to external organisations or individuals working on our behalf. Staff who do not comply with the policy may face disciplinary action.
- 3.2 It applies to all data that Community Links holds relating to identifiable individuals, even if that information technically falls outside of the data protection act.

3. Applicable legislation

- 3.1 This policy meets the requirements of the:
 - Data Protection Act 2018 (DPA 2018)
 - UK General Data Protection Regulations (UK GDPR). The EU GDPR was incorporated into UK legislation with some amendments by the Data Protection, Privacy and Electronic Communications (Amendments) (EU Exit) Regulations 2020
 - Freedom of Information Act 2000
- 3.2 This policy is also based on and complies with guidance published by the Information Commissioner's Office (ICO)

4. Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, living individual. This may include the individual's: • Name (including initials)

	• Identification number • Location data • Online identifier, such as a username • It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special category data	Previously called 'Sensitive Personal data', this is personal data which is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • Health – physical or mental • Sex life or sexual orientation
Data processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, sharing, disseminating, erasing or destroying. Processing can be automated or manual.
Automated processing	Any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. An example of automated processing includes profiling and automated decision making. Automatic decision making is when a decision is made which is based solely on automated processing (without human intervention) which produces legal effects or significantly affects an individual. Automated decision making is prohibited except in exceptional circumstances.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure or, or access to, personal data
Data Protection Impact Assessments (DPIA)	A tool used to identify risks in data processing activities with a view to reducing them.
Criminal Records Information	Personal information relating to criminal convictions and offences, allegations, proceedings, and related security measures.

5. Data Controller and Processor

5.1 Community Links determines the purposes and means of processing personal data and special category data and is therefore a data controller. Community Links provides services under contract to third parties such as Lancashire County Council which may determine how some data is to be processed; therefore Community Links is also a data processor.

5.2 Community Links is registered with the ICO under registration number ZB852249

6. Roles and responsibilities

Term	Definition
Directors	• Overall responsibility for ensuring Community Links complies with all relevant data protection obligations
Data Protection Officer (DPO)	The Data Protection Officer, steve.woods@mycommunitylinks.com is responsible for: • Keeping the Directors updated about data protection responsibilities, risks and issues • Reviewing all data protection procedures and related policies, in line with agreed schedule • Arranging data protection training and advice for all employees and contractors covered by this policy • Handling data protection questions from employees and contractors and any other identifiable individual covered by this policy • Dealing with requests from identifiable individuals to see the data Community Links holds about them (also called 'subject access requests') • Checking and approving any contracts or agreements with third parties that may handle Community Links's sensitive data • Approving any data protection statements attached to communications such as emails or letters • Addressing data protection queries from journalists or media • Where necessary, working with employees or contractors to ensure marketing initiatives and literature abide by data protection principles • Overseeing implementation of this policy, monitoring our compliance with data protection law, developing related policies and guidelines. • Provide annual report directly to the Board, and where relevant, report to the board advice and recommendations on data protection issues.
All staff	• Collect, store and process any personal data in accordance with this policy • Informing Community Links of any changes to their personal data, such as a change of address • Contacting the DPO in the following circumstances: • With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure • If they have concerns this policy is not being followed

	• If they are unsure whether or not they have a lawful basis to use personal data in a particular way • If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside UK • If there has been a potential or known data breach • Whenever they are engaging in a new activity that may affect the privacy rights of individuals • If they need help with any contracts or sharing personal data with third parties
--	--

7. Data protection principles

7.1 The UK GDPR sets out seven key principles:

1. Lawfulness, fairness and transparency. We only process personal data where we have one of the six lawful bases (legal reasons) to do so:
 - Fulfil a contract
 - The individual has freely given clear consent
 - Comply with a legal obligation
 - Ensure the vital interests of the individual; or another person (ie; to protect someone's life)
 - For the legitimate interests of Community Links
 - To perform a task in the public interest
2. Purpose limitation. We collect personal data for specified, explicit and legitimate reasons.
3. Data minimisation. We collect data which is adequate and relevant to the purpose.
4. Accuracy. We ensure data is accurate and current.
5. Storage limitation. We do not hold data for longer than is necessary.
6. Integrity and confidentiality (security). We maintain appropriate technical, organisational and people controls to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage
7. Accountability. We monitor compliance.

8. Sharing Personal Data

8.1 Community Links will generally not share personal data with third parties unless certain safeguards and contractual arrangements have been put in place, but there are certain circumstances where we may be required to do so. These include but are not limited to situations where:

- We are required either by law or in the best interests of our learners or staff to pass information onto external authorities for example, emergency services, Ofsted, Awarding organisations or Department of Health. These authorities are up to date with data protection law and have their own policies relating to the protection of any data that they receive or collect.
- There is an issue with a learner that puts the safety of our staff or learners at risk
- Our suppliers or contractors need data to enable us to provide services – for example, our IT service providers. Where this is the case, we will:
 - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with UK data protection law
 - Establish a contract with the supplier or contractor to ensure the fair and lawful processing of any personal data we share

- Only share data that the supplier or contractor needs to carry out their service

8.2 We will share personal data with law enforcement and government bodies where we are legally or contractually required to do so. We may share personal data with emergency services to help them to respond to an emergency situation that affects any of our learners or staff.

8.3 If there was need to transfer personal data internationally, we will do in accordance with UK data protection law. It will not be transferred outside of the European Economic Area (EEA) unless that country or territory also ensures an appropriate level of protection

9. Subject Access Requests

9.1 See Appendix 1

10. Other data protection rights of the individual

10.1 Individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Object to processing which has been justified on the basis of public interest, official authority or legitimate interests
- Challenge decisions based solely on automated decision making or profiling (i.e. making decisions or evaluating certain things about an individual based on their personal data with no human involvement)
- Be notified of a data breach (in certain circumstances)
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

10.2 Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DP).

11. Employee and Contractor Obligations

11.1 Employees and Contractors may have access to the personal data of other members of staff, suppliers or learners of Community Links in the course of their employment or engagement. If so, Community Links expects those employees to help meet our data protection obligations to those individuals. Specifically, staff must: -

- Only access the personal data that they have authority to access, and only for authorised purposes
- Only allow others to access personal data if they have appropriate authorisation;
- Keep personal data secure.
- Not to share the data
- Review data regularly to ensure currency
- Not remove personal data or devices containing personal data from Community Links premises unless appropriate security measures are in place (such as pseudonymisation, encryption, password protection) to secure the information
- Not store personal information on local drives.

- Make sure that a data subject (identifiable individual) knows how their data is being used and how to exercise their rights
- Seek support the DPO if you have any questions about this policy

12. Biometric recognition systems

- 12.1 Community Links does not use any biometric recognition systems such a finger print to access areas of a site. However, if we were to use such a system in the future, we will ensure we will comply with the requirements of the Protection of Freedoms Act 2012.

13. Data protection by design and default

- 13.1 We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:
- Appointing a suitably experienced DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their knowledge
 - Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out above
 - Completing data protection impact assessments where our processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies
 - Integrating data protection into internal documents including this policy, any related policies and privacy notices
 - Training members of staff on data protection law, this policy, any related policies and any other data protection matters
 - Conducting reviews and/or internal audits to test compliance
 - Appropriate safeguards being put in place if we transfer any personal data outside of the UK, where different data protection laws may apply
 - Maintaining records of our processing activities
 - For the benefit of data subjects, making available the name and contact details of our DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
 - For all personal data that we hold, maintaining an internal record of the type of data, type of data subject, how and why we are using the data, any third-party recipients, any transfers outside of the UK and the safeguards for those, retention periods and how we are keeping the data secure

14. Data breaches

- 14.1 See Appendix 2

15. Monitoring

- 15.1 The DPO is responsible for monitoring and reviewing this policy. The DPO is responsible for providing independent scrutiny of the policy through audits.

16. Removable Media Policy

To reduce the risk of data loss, corruption, or unlawful disclosure associated with removable media, Community Links implements the following controls:

16.1 Purpose

This section provides clear rules for the use, management, and monitoring of removable media to prevent data breaches and ensure compliance with UK GDPR and internal security standards.

16.2 Approved Use

- Removable media should only be used when alternative, more secure methods (e.g., encrypted cloud storage or secure file transfer systems) are not suitable.
- Any use must be authorised by the DPO or an appointed manager.

16.3 Security Requirements

All removable media used for Community Links data must:

- Be encrypted and password-protected.
- Be registered with the IT service provider so usage can be monitored.
- Be labelled with a unique identifier for tracking.
- Be stored in locked cabinets when not in use.

16.4 Restrictions

Staff must not:

- Use personal or unapproved removable media on Community Links equipment.
- Use removable media to circumvent secure storage systems.
- Store special category data on removable media unless absolutely unavoidable and authorised in writing.

16.5 Transporting Removable Media

When transporting removable media containing personal data:

- Devices must remain with the staff member at all times.
- They must not be left in vehicles or unsecured environments.
- They should be transported in a protective case.

16.6 Disposal

When removable media reaches the end of its life or is no longer required:

- It must be returned to IT for secure destruction.
- Deletion of data must follow approved secure erasure techniques.

16.7 Monitoring and Audit

- Use of removable media will be monitored by the IT service provider.
- Regular audits will be conducted to ensure compliance

APPENDIX 1 - Data Breach Policy and Procedure

1. Purpose

- 1.1 The purpose of this document is to detail how to report a data breach and the steps Community Links undertake when managing a data breach.

2. Definition and Terms

Term	Definition
Data Breach	An incident that results in confirmed disclosure of data to an unauthorised party. Examples of disclosure: • Accidental or deliberate disclosure of information to unauthorised individuals • Sending a sensitive email to “all staff” by mistake • Data sent to an unintended or unauthorised recipient • Data posted on the internet, either accidentally or intentionally • Conversation with an inappropriate person or in an inappropriate place (e.g. corridor or stairwell) • Theft or loss of paper records of data • Theft or loss of any of Community Links’s computer equipment, mobile phone, or removable media with Community Links data stored on it • Missing learner records, correspondence and files

3. Policy

- 3.1 All Community Links employees have a responsibility to report security incidents and data breaches immediately. This obligation extends to external organisations contracted to support or access Community Links information systems. Examples of what constitutes a data breach can be seen in definitions and terms above.

Managing data breach

- 3.2 Community Links manages data breaches following these five steps:

- Reporting the incident
- Containment and recovery
- Assessment of ongoing risk
- Notification of breach
- Evaluation and response

3.3 Reporting the Incident

- Any breach must be reported within 1 hour of the possible breach being identified. Community Links has 72 hours after a potential breach is identified in which to contain the situation, assess the risks to data subjects and determine whether the breach is reportable to the Information Commissioner’s Office.
- Data breaches must be reported to line manager and DPO either via phone or email.

- Incidents can be reported in confidence
- When reporting incidents it is important that the following information is captured:
 - Incident Date/Time
 - Department
 - Work location/site
 - Contact details phone etc
 - Type of incident
 - Description about the incident including detail about what information is missing and what sort of personal information is contained in the missing records.
- When an incident is reported, a member of the senior management team will also be informed.

3.4 Containment and Recovery

- If an employee has lost or mislaid a file or paperwork, time may be granted to search to recover it.
- The incident will be investigated as soon as Community Links is made aware of the situation. Hardware, logs and records may be analysed by any authorised representative of Community Links. Information and data may be gathered as evidence to support containment, recovery and any possible disciplinary or legal action. It is essential during the course of these investigations that confidentiality is maintained at all times.
- The information regarding any incident which has been provided will be recorded as an incident (a Data Breach).
- Data security breaches require not just an initial response to investigate and contain the situation but also a recovery plan including, where necessary, damage limitation. This will often involve input from specialists across Community Links including the IT Service Provider and in some cases contact with external stakeholders and suppliers.

3.5 We will:

- Decide on who should take the lead on investigating the breach and ensure they have the appropriate resources.
- Establish who needs to be made aware of the breach and inform them of what they are expected to do to assist in the containment exercise. This could be isolating or closing a compromised section of the network, finding a lost piece of equipment or simply changing the access codes at the front door.
- Establish whether there is anything you can do to recover any losses and limit the damage the breach can cause. As well as the physical recovery of equipment, this could involve the use of backups to restore lost or damaged data or ensuring that staff recognise when someone tries to use stolen data to access accounts
- Where appropriate, inform the police.

3.6 Assessing the Risks

Some data security breaches will not lead to risks beyond possible inconvenience to those who need the data to do their job. An example might be where a laptop is irreparably damaged but its files were backed up and can be recovered, albeit at some cost to Community Links. While these types of incidents can still have significant consequences the risks are very different from those posed by, for example, the theft of a customer database, the data on which may be used to commit identity fraud

3.7 Before deciding on what steps are necessary further to immediate containment, we will assess the risks which may be associated with the breach. This will include an

assessment of potential adverse consequences for individuals, how serious or substantial these are and how likely they are to happen. Our assessment will consider:

- What type of data is involved?
- How sensitive is it? Some data is sensitive because of its very personal nature (e.g. health records) while other data types are sensitive because of what might happen if it is misused (e.g. bank account details)
- If data has been lost or stolen, are there any protections in place such as encryption?
- What has happened to the data? If data has been stolen, might it be used for purposes which are harmful to the individuals to whom the data relates. If it has been damaged, this poses a different type and level of risk
- Regardless of what has happened to the data, what could the data tell a third party about the individual? Sensitive data could mean very little to an opportunistic laptop thief while the loss of apparently trivial snippets of information could help a determined fraudster build up a detailed picture of other people
- How many individuals' personal data are affected by the breach? It is not necessarily the case that the bigger risks will accrue from the loss of large amounts of data but is certainly an important determining factor in the overall risk assessment
- Who are the individuals whose data has been breached? Whether they are staff, customers, clients or suppliers, for example, will to some extent determine the level of risk posed by the breach and, therefore, Community Links's actions in attempting to mitigate those risks
- What harm can come to those individuals? Are there risks to physical safety or reputation, of financial loss or a combination of these and other aspects of their life?
- Are there wider consequences to consider such as a risk to public health or loss of public confidence in an important service you provide?
- If individuals' bank details have been lost, we will consider contacting the banks themselves for advice on anything they can do to help you prevent fraudulent use.

3.8 Notification of breaches

Informing people and organisations that Community Links has experienced a data security breach is an important element in our breach management strategy. Informing people about a breach is not however an end in itself; notification will have a clear purpose - to enable individuals who may have been affected to take steps to protect themselves and/or to allow the appropriate regulatory bodies to perform their functions, provide advice and deal with complaints.

3.9 When considering whether to notify, Community Links will consider:

- Are there any legal or contractual requirements? Community Links may have an obligation to notify prime contractors and the Information Commissioner in certain circumstances.
- Can notification help Community Links meet its security obligations?
- Can notification help the individual? For example, giving them opportunity to cancel a credit card or change a password?
- If a large number of people are affected, or there are very serious consequences, we will notify the ICO.
- Consideration will be given to how notification can be made appropriate for particular groups of individuals, for example, if Community Links needs to notify vulnerable adults or children.

- 3.10 Community Links will consider the danger of 'over notifying'. Not every incident will warrant notification and notifying too many people unnecessarily may well cause disproportionate enquiries and work. In practical terms, Community Links will consider who to notify, what is going to be told to them and how the message will be communicated. This will depend to a large extent on the nature of any breach but the following points will be considered:
- Whether an appropriate regulatory body expects notification. The ICO should only be notified when the breach involves personal data.
 - There are a number of different ways to notify those affected so we will determine the most appropriate one, bearing in mind security and urgency.
 - Any notification will include a description of how and when the breach occurred, what data was involved, details of what action has been taken to respond to the risks posed by the breach.
- 3.11 When notifying individuals they will be given specific and clear advice on the steps they can take to protect themselves and also what Community Links is willing to do to help them. They will be provided with a way in which they can contact Community Links for further information or to ask questions.
- 3.12 If the ICO is notified, Community Links will include details of the security measures in place such as encryption and, where appropriate, details of the security procedures in place at the time the breach occurred. The ICO will also be informed if the media are aware of the breach so that they can manage any increase in enquiries from the public.
- 3.13 Consideration will also be given to whether to notify third parties such as the police, insurers, professional bodies, and bank/credit card companies who can assist in reducing loss to individuals.

4. Evaluation and Response

It is important to Community Links that we evaluate the effectiveness of our response. The following points will be considered in our evaluation:

- Re-assess what personal data is held and where and how it is stored. Dealing with a data security breach is much easier if you know which data are involved
- Establish where the greatest risks lie
- Re-appraise any weak points in existing security measures
- Evaluation of effectiveness of information security policies and staff awareness

APPENDIX 2 - Data Subject Access Requests (SARs)

1. Purpose

- 1.1 This document sets out the rights of data subjects to make a subject access request and the procedure we use when acting on such a request.

2. Introduction

- 2.1 Under Data Protection law, data subjects have a general right to find out whether Community Links holds or processes personal data about them, to access that data, and to be given supplementary information. This is known as the right of access or the right to make a data subject access request (SAR). The purpose of the right is to enable the individual to be aware of and verify the lawfulness of the processing of personal data that Community Links is undertaking. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- Where relevant, the existence of the right to request rectification, erasure or restriction, or to object to such processing
- The right to lodge a complaint with the ICO or another supervisory authority
- The source of the data, if not the individual themselves
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual
- The safeguards provided if the data is being transferred internationally

- 2.2 Subject Access Requests can be submitted in any form, but we may be able to respond to requests more quickly if they are made in writing and include:

- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested

If staff receive a subject access request in any form they must immediately forward it to the DPO.

3. Policy

- 3.1 When responding to requests, we:
- Will assure ourselves that the individual making the request has the right to access the information being requested. We may ask the individual to provide two forms of identification and contact the individual via phone to confirm the request was made
 - Will respond without delay and within one month of receipt of the request (or receipt of the additional information needed to confirm identity, where relevant)
 - Will provide the information free of charge

- May tell the individual we will comply within three months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within one month, and explain why the extension is necessary
- 3.2 We may not disclose information for a variety of reasons, such as if it:
- Might cause serious harm to the physical or mental health of an individual
 - Would reveal that a person is being or has been abused, or is at risk of abuse, where the disclosure of that information would not be in the person's best interests
 - Would include another person's personal data that we cannot reasonably anonymise, and we do not have the other person's consent and it would be unreasonable to proceed without it
 - Is part of certain sensitive documents, such as those related to crime, immigration, legal proceedings or legal professional privilege, management forecasts, negotiations, confidential references, or exam/test scripts
- 3.3 If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee to cover administrative costs. We will take into account whether the request is repetitive in nature when making this decision.
- 3.4 When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO or they can seek to enforce their subject access right through the courts.

4. Procedure

- 4.1 Failure to comply with the right of access under UK GDPR puts both staff and Community Links at potentially significant risk and so we take compliance with this policy very seriously.

Recognising a Subject Access Request

- 4.2 A data subject access request is a request from an individual (or from someone acting with the authority of an individual, e.g., a solicitor):
- for confirmation as to whether Community Links processes personal data about him or her and, if so
 - for access to that personal data
 - and/or certain other supplementary information
- 4.3 A valid SAR can be made in writing (by letter, email, WhatsApp, text) or verbally (e.g., during a telephone conversation).
- 4.4 The request may refer to the UK GDPR and/or to 'data protection' and/or to 'personal data' but does not need to do so in order to be a valid request. For example, a letter which states '*please provide me with a copy of information that Community Links holds about me*' would constitute a data subject access request and should be treated as such.
- 4.5 A data subject is generally only entitled to access their own personal data and not information relating to other people.

Making a Subject Access Request

- 4.6 Whilst there is no requirement to do so, we encourage any individuals who wish to make such a request to make the request in writing, detailing exactly the personal data

being requested. This allows Community Links to easily recognise that you wish to make a data subject access request and the nature of your request.

- 4.7 If the request is unclear or vague we may have to clarify the scope of the request which may delay the start of the time period for dealing with the request.

Receiving a Data Subject Access Request

- 4.8 All data subject access requests should be immediately directed to the DPO (steve.woods@mycommunitylinks.com). There are limited timescales within which Community Links must respond to a request and any delay could result in failing to meet those timescales, which could lead to enforcement action by the Information Commissioner's Office (ICO) and/or legal action by the affected individual.

Acknowledging the Request

- 4.9 When receiving a SAR, Community Links will acknowledge the request as soon as possible and inform the requester about the statutory deadline (one calendar month) to respond to the request. In addition to acknowledging the request, we may ask for:
- proof of ID
 - further clarification about the requested information
 - if it is not clear where the information shall be sent, we will clarify what address/email address to use when sending the requested information (we are likely to cross-reference this information as part of our checks) and/or
 - consent (if requesting third party data).

Verifying the identity of a requester

- 4.10 Before responding to a SAR, we will take reasonable steps to verify the identity of the person making the request. In the case of current employees, this will usually be straightforward.
- 4.11 We are entitled to request additional information from a requester in order to verify whether the requester is in fact who they say they are. Where we have reasonable doubts as to the identity of the individual making the request, evidence of identity may be sought by production of a passport, driving licence, recent utility bill with current address, birth/marriage certificate, credit card or a mortgage statement.
- 4.12 If an individual is requesting a large amount of data, we may ask the requester for more information for the purpose of clarifying the request, but the requester shall never be asked why the request has been made. We will let the requestor know as soon as possible where more information is needed before responding to the request.
- 4.13 In both cases, the period of responding begins when the additional information has been received. If Community Links does not receive this information, we will be unable to comply with the request.

Requests made by third parties

- 4.14 Community Links needs to be satisfied that a third party making a request is entitled to act on behalf of the individual, but it is the third party's responsibility to provide evidence of this entitlement. This might be a written authority to make the request or it might be a more general power of attorney. We may also require proof of identity in certain circumstances.

- 4.15 If Community Links is in any doubt or has any concerns as to providing the personal data of the data subject to the third party, then it should provide the information requested directly to the data subject. It is then a matter for the data subject to decide whether to share this information with any third party.

Fee For Responding to a DSAR

- 4.16 Community Links will usually charge £10 administrative fee to deal with a SAR. Where a request is considered to be manifestly unfounded or excessive an additional fee to cover administrative costs may be requested. If a request is considered to be manifestly unfounded or unreasonable Community Links will inform the requester why this is considered to be the case and the fee which will be charged for complying with the request.
- 4.17 A fee may also be requested in relation to repeat requests for copies of the same information. In these circumstances a reasonable fee will be charged taking into account the administrative costs of providing the information.
- 4.18 If a fee is requested, the period of responding begins when the fee has been received.

Time Period for Responding to a SAR

- 4.19 Community Links has one calendar month to respond to a SAR. This will run from the day that the request was received or from the day when any additional identification or other information requested is received, or payment of any required fee has been received.
- 4.20 The circumstances where Community Links is in any reasonable doubt as to the identity of the requester, this period will not commence unless and until sufficient information has been provided by the requester as to their identity and in the case of a third party requester, the written authorisation of the data subject has been received.
- 4.21 The period for response may be extended by a further two calendar months in relation to complex requests. What constitutes a complex request will depend on the particular nature of the request. The DPO must always be consulted in determining whether a request is sufficiently complex as to extend the response period.
- 4.22 Where a request is considered to be sufficiently complex as to require an extension of the period for response, we will notify the requester within one calendar month of receiving the request, together with reasons as to why this extension is considered necessary.

Information to be provided in response to a request

- 4.23 The individual is entitled to receive access to the personal data we process about him or her and the following information:
- the purpose for which we process the data
 - the recipients or categories of recipient to whom the personal data has been or will be disclosed, in particular where those recipients are in third countries or international organisations
 - where possible, the period for which it is envisaged the personal data will be stored, or, if not possible, the criteria used to determine that period

- the fact that the individual has the right:
- to request that Community Links rectifies, erases or restricts the processing of his personal data
- to object to its processing
- to lodge a complaint with the ICO
- where the personal data has not been collected from the individual, any information available regarding the source of the data
- any automated decision we have taken about him or her together with meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for him or her.

4.24 The information should be provided in a way that is concise, transparent, easy to understand and easy to access using clear and plain language, with any technical terms, abbreviations or codes explained. The response shall be given in writing if the SAR was made in writing in a commonly used electronic format.

4.25 The information that Community Links is required to supply in response to a SAR must be supplied by reference to the data in question at the time the request was received. However, as Community Links has one month in which to respond we are allowed to take into account any amendment or deletion made to the personal data between the time the request is received and the time the personal data is supplied if such amendment or deletion would have been made regardless of the receipt of the SAR. Therefore, Community Links is allowed to carry out regular housekeeping activities even if this means deleting or amending personal data after the receipt of a SAR. Community Links is not allowed to amend or delete data to avoid supplying the data.

How to Locate Information

4.26 The personal data Community Links might need to provide in response to a SAR may be located in different electronic and paper filing systems. This is why it is important to identify at the outset the type of information requested so that the search and retrieval can be focused. Depending on the type of information requested, we may need to search all or some of the following:

- electronic systems, e.g., databases, networked and non-networked computers, servers, customer records, human resources system, email data, back up data, CCTV
- manual filing systems in which personal data is accessible according to specific criteria, e.g., chronologically ordered sets of manual records containing personal data
- data systems held externally by our data processors
- occupational health records
- pensions data
- insurance benefit information.

We will search these systems using the individual's name, employee number or other personal identifier as a search determinant.

Protection of Third Parties - Exemptions to the Right of Subject Access

4.27 There are circumstances where information can be withheld pursuant to a SAR. These specific exemptions and requests should be considered on a case by case basis.

- 4.28 We will consider whether it is possible to redact information so that this does not identify third parties. If their data cannot be redacted (for example, after redaction it is still obvious who the data relates to) then we do not have to disclose personal data to the extent that doing so would involve disclosing information relating to another individual (including information identifying the other individual as the source of information) who can be identified from the information unless:
- the other individual has consented to the disclosure
 - it is reasonable to comply with the request without that individual's consent.
 - In determining whether it is reasonable to disclose the information without the individual's consent, all of the relevant circumstances will be taken into account, including:
 - the type of information that they would disclose
 - any duty of confidentiality they owe to the other individual
 - any steps taken to seek consent from the other individual
 - whether the other individual is capable of giving consent, and
 - any express refusal of consent by the other individual
- 4.29 It needs to be decided whether it is appropriate to disclose the information in each case. This decision will involve balancing the data subject's right of access against the other individual's rights. If the other person consents to the Community Links disclosing the information about them, then it would be unreasonable not to do so. However, if there is no such consent, Community Links must decide whether to disclose the information anyway. If there are any concerns in this regard then the DPO should be consulted.

Other Exemptions to the Right of Subject Access

- 4.30 In certain circumstances Community Links may be exempt from providing some or all of the personal data requested. These exemptions are described below and should only be applied on a case-by-case basis after a careful consideration of all the facts.
- *Crime detection and prevention:* Community Links does not have to disclose any personal data being processed for the purposes of preventing or detecting crime; apprehending or prosecuting offenders; or assessing or collecting any tax or duty.
 - *Confidential references:* Community Links does not have to disclose any confidential references given to third parties for the purpose of actual or prospective:
 - education, training or employment of the individual;
 - appointment of the individual to any office; or
 - provision by the individual of any service
 - This exemption does not apply to confidential references that Community Links receives from third parties. However, in this situation, granting access to the reference may disclose the personal data of another individual (i.e., the person giving the reference), which means that we must consider the rules regarding disclosure of third-party data set out above before disclosing the reference.
 - *Legal professional privilege:* Community Links does not have to disclose any personal data which is subject to legal professional privilege.
 - *Management forecasting:* Community Links does not have to disclose any personal data processed for the purposes of management forecasting or management planning to assist us in the conduct of any business or any other activity.
 - *Negotiations:* Community Links does not have to disclose any personal data consisting of records of intentions in relation to any negotiations with the individual where doing so would be likely to prejudice those negotiations.

Refusing to Respond to a Request

- 4.31 Community Links can refuse to comply with a request if the request is manifestly unfounded or excessive, taking into account whether the request is repetitive in nature. If a request is found to be manifestly unfounded or excessive, Community Links can:
- request a "reasonable fee" to deal with the request; or
 - refuse to deal with the request.

Record Keeping

- 4.32 A record of all subject access requests shall be kept by the DPO. The record shall include the date the SAR was received, the name of the requester, what data Community Links sent to the requester and the date of the response.

END

Version Control

Version history	Content Changed
1 – Sep 2024	Policy produced
2 – 01/03/2025	• Reviewed
3 – 25/10/2025	• Legislation and regulation updated • Breach process expanded and moved to separate appendix • Subject Access Request process expanded and moved to separate appendix
4 – 23/10/26	• Policy Agreed

Review and Ratification

Next Review Date	Reason for Review
October 2027	Full Review