

Data Protection Policy



Policy Date: November 2018

Reviews

Date	Key changes (if any)	Next review
August 2023	Glossary of Terms added	August 2024
August 2025	• Data Protection Act details changed • The policy is combined with the data protection section in the Employee Handbook • Accountability and transparency added to the Principles list	August 2026
September 2026	Updated: • Right to information about decision making • Data Protection Officer to Data Protection Manager	September 2027

Introduction

In this policy:

- **Act** means the Data Protection Act 2018.
- **Data** means information that can be stored electronically or on paper.
- **Data processor** means another organisation, or person who doesn't work for us, that processes the personal data we hold on our behalf.
- **Data Protection Manager** is Sule Kangulec.
- **GDPR** means the General Data Protection Regulation.
- **ICO** means the Information Commissioner's Office (ico.org.uk)
- **Individual** means anyone we hold personal data on (including our staff).
- **Personal data** means data we hold (factual or opinion based) that can directly or indirectly identify a living individual (e.g. their name, address or date of birth). Includes sensitive personal data.
- **Personal data breach** means the loss, unauthorised access, disclosure or acquisition of personal data or any act or omission that compromises the security, confidentiality, integrity or availability of the personal data or the physical, technical, administrative or organisational safeguards that we or our third-party service providers put in place to protect it.
- **Privacy notice** means a document or other form of notice containing information on how we handle an individual's personal data when we collect it.
- **Processing** or **processed** means any activity involving the use of personal data. This includes obtaining, recording or holding it and carrying out tasks with it including using, disclosing, retrieving, accessing, organising, amending or erasing it.
- **Sensitive personal data** means special category data, plus information about any committed or alleged criminal offences including the outcome of any criminal proceedings.

- **Special category data** means information about an individual's racial or ethnic origin, political opinion, trade union membership, religion, philosophical beliefs, physical or mental health, sexual orientation or sex life, genetics or biometrics.
- **Staff** means all individuals working for us at every level or grade, whether they're directors, officers, employees, workers, contractors, consultants, agency workers, volunteers, trainees or on work experience.
- **Stakeholders** mean any private or public commercial organisations (including charities and 'not for profit' bodies) that provide services to us or on our behalf including, but not limited to, subcontractors, agents, contractors, advisors, suppliers and business and joint venture partners.
- **Explicit consent** means freely given, specific and informed agreement by an Individual/Service User in the processing of personal information about them.
- **Notification** means paying the annual data protection fee to the Information Commissioner's Office (ICO), as required under the Data Protection Regulations 2018.

We'll process all personal data we hold in accordance with the Act and the GDPR. Personal Data is subject to the legal safeguards specified in the GDPR. While staff work for us we'll collect and process their personal data for personnel, management and administrative purposes and to enable us to meet our legal obligations as an employer.

In the course of our business, we'll also collect and process personal data that we receive from various organisations. This may include data on individuals who currently, or used to, work for our clients or customers, business partners and stakeholders.

The purpose of this policy is to explain individuals' data protection rights, how we'll handle their personal data and how our staff must handle the personal data of others.

Data may be obtained by completing forms or by corresponding with us by mail, phone, email or social media. It could also be obtained from other sources, such as from our business partners and stakeholders.

Staff should be aware that they could be criminally liable if they knowingly or recklessly disclose personal data in breach of the GDPR. A serious data protection breach is a disciplinary offence. If a member of staff accesses another staff member's personnel records without authority, this will be a gross misconduct offence.

Policy statement

As a data controller we must fully comply with our legal obligations under the Act and the GDPR. Failure to do so may result in criminal prosecution and/or a fine by the ICO. We will only process personal data:

- That we legitimately require for the purposes of our business and our employment relationship with our staff
- Using one or more of the lawful grounds stated in the GDPR/the Act
- After having informed the individual of what that purpose is, using clear and plain language.

Data Protection Policy



We'll securely store all processed data, and regularly review it to ensure it remains complete, accurate and necessary for the purpose for which we hold it. If appropriate we'll securely delete it in accordance with our retention criteria.

We'll make all individuals aware of the risks, rules, safeguards and rights in relation to processing their data and how they can exercise their rights. We'll do this using various documents (such as this policy) to demonstrate our compliance with the data protection principles.

We'll provide training in data protection compliance to all staff who need it to perform their roles.

Data protection manager's functions and duties

The Data Protection Manager will:

- Inform and advise us and our staff of any obligations under the GDPR and the Act,
- Monitor and review this policy and make sure it's complied with,
- Cooperate with the ICO, and
- Be the first point of contact for the ICO and for any individual regarding data protection.

Staff should contact the Data Protection Manager if they have any questions about the operation of this policy, such as if they:

- Need to draft a privacy notice,
- Are unsure of the lawful basis to process personal data,
- Need to get an individual's consent to process their data,
- Plan to use personal data for purposes other than that which it was collected for,
- Are unsure how to transfer or share personal data with a third party,
- Are unsure what security or other measures they need to implement to protect the personal data we hold,
- Need help with any contracts or other information about sharing personal data with third parties,
- Are unsure about the retention period for data that is no longer needed,
- Have received a 'data subject access request' or any request by an individual to exercise rights under the GDPR,
- Need help to perform a data privacy impact assessment,
- Plan to conduct direct marketing activities,
- Plan to use automated processing including profiling or automated decision making,
- Believe or know that a personal data breach has happened,
- Believe or know that this policy has been breached.

The data protection principles

The following list is central to the Act and the GDPR. It must be applied at all times when processing personal data. Personal data must be:

- Processed lawfully, fairly and transparently, i.e. the information given to the individual must be easy to access and read, using clear and plain language,
- Collected only for specified, explicit and legitimate purposes and not processed in a way that's incompatible with those purposes, i.e. processed only if there is no other way to fulfil the purpose,
- Adequate, relevant and limited to what is necessary for the reason for processing it, i.e. data can't be collected for general or future use,
- Accurate and, where necessary, kept up to date, i.e. every reasonable step must be taken to ensure that any inaccurate data (taking into consideration the reason why it is being processed) is erased or corrected without delay,
- Kept in a format that identifies an individual for no longer than is necessary for the purposes of the processing, unless the data is being processed only with the intention of archiving in the public interest, scientific or historical research or statistical purposes (subject to appropriate technical and organisational procedures being implemented). I.e. the personal data shouldn't be kept for longer than necessary,
- Processed in a way that ensures it'll be protected using appropriate security (using technical or organisational measures) including protection against unauthorised or unlawful processing, accidental loss and destruction or damage.

We must both comply with these principles at all times when handling personal data. We must also be able to demonstrate that we comply with them.

Community Matters will, through appropriate management and strict application of criteria and controls:

- Observe fully conditions regarding the fair collection and use of information
- Meet its legal obligations to specify the purposes for which information is used
- Collect and process appropriate information, and only to the extent that it is needed to fulfil its operational needs or to comply with any legal requirements
- Ensure the quality of information used
- Ensure that the rights of people about whom information is held can be fully exercised
- Take appropriate technical and organisational security measures to safeguard personal information
- Treat people justly and fairly whatever their age, religion, disability, gender, sexual orientation or ethnicity when dealing with requests for information
- Set out clear procedures for responding to requests for information

Community Matters will ensure that any disclosure of personal data complies with a lawful basis for processing under UK GDPR, such as legal obligation or legitimate interests.

Processing personal data fairly and the lawful grounds for processing

To ensure that an individual's privacy is protected, only personal data that we legitimately require for the purposes of our business and the employment relationship with our staff should be processed, using one or more of the following lawful grounds specified in the GDPR:

Consent

- This should only be used if we cannot rely on one of the other lawful grounds.
- This can only be used where an individual has freely given clear and unambiguous consent for us to process their personal data for a specific purpose. Before the processing begins, we must inform them in clear and plain language of what the purpose is and that they can withdraw consent at any time.
- It must be a positive action that, wherever possible, is given by a very clear and specific written statement (i.e. not just an action).
- Wherever possible we'll inform the individual from the start of all the purposes for which consent is required, as it'll have to be re-obtained if we later need the personal data for a different purpose.
- We **must not** get consent using pre-ticked boxes, silence or when we have an unequal bargaining position with the individual (e.g. when we are in a position of power over the individual).
- If we're processing the individual's personal data for automated decision making or cross-border data transfers, we'll usually need to get their clear, specific written consent, unless we can rely on another lawful ground.
- We'll keep evidence of the consent so that we can demonstrate compliance.

Performance of a contract

This can be used where we have a contract with an individual, or they've asked us to take specific steps before entering into a contract and the processing is necessary to fulfil our obligations under it.

Legal obligation

This can be used where we must comply with a statute (UK and EU or a regulatory requirement where it's supported by statute), a court order or common (case) law. It doesn't include contractual obligations.

We should identify the obligation by referring to either the specific legal provision or to an appropriate resource that sets it out clearly (e.g. a government website or to industry guidance).

Legitimate interests

This can be used where the processing is necessary for our legitimate interests or those of a third party, unless there is a good reason to protect the individual's personal data that overrides those legitimate interests. Extra care must be taken if processing data on children.

Before using legitimate interests to process data, we must conduct a 'legitimate interests assessment' to balance our interests in having the data processed against the rights of the individual. This assessment must be done for each legitimate purpose and usually by the HR manager with help from the Data protection manager. The extent of this assessment depends on what type of data is being processed.

The GDPR states that the processing will be for a legitimate interest if, for example, the processing is shown to be necessary for:

- Fraud prevention
- Network and information security
- Preventing possible criminal acts or threats to public security. For these purposes the legitimate interests assessment will be brief.

The GDPR also states that the following purposes for processing might be legitimate:

- Processing staff or client data
- Direct marketing
- Intra-group administrative transfers.

For these purposes the legitimate interests assessment will need to ensure that the individual's rights and interests are fully considered and protected.

We will use a privacy notice to tell individuals that we're relying on legitimate interests to process their data. This will state why we're processing the data and why it's necessary.

Vital interests

This can be used only if the processing is necessary to protect the individual's life or the life of another person where their personal data can't be lawfully processed in another way. This is likely to be used rarely. Examples include:

- Providing medical information where someone has life-threatening injuries
- Using a parent's personal data to protect the life of their child.

Public interest

This can be used where it's necessary for the performance of a task carried out in the public interest (e.g. detecting crime or fraud) or in exercising any official authority we might have.

Being transparent

We'll only process personal data using one or more of the lawful grounds stated in the GDPR/the Act.

Data Protection Policy



We must provide detailed and specific information to an individual about how we will handle their data. We will usually do this by giving them a privacy notice.

The contents of the privacy notice will depend on whether the data is collected directly from the individual or from a third party.

Staff **must** only use our privacy notice templates (if any) when drafting a privacy notice for an individual.

Limiting the purpose

We'll only process personal data **after** informing the individual of what the purpose is, using clear and plain language. This means staff **must not**:

- Process it in any way that's incompatible with that purpose
- Use it for any other purpose.

Minimising the amount of data we hold

We'll only collect and process personal data that we legitimately require for the purposes of our business and our employment relationship with our staff. Personal data must only be:

- Processed as required by a staff member's job duties
- Collected only to the extent that is necessary for the stated purpose
- Kept no longer than is necessary for the stated purpose, ensuring that it'll be either securely deleted or pseudonymised (using artificial identifiers - or pseudonyms - to separately store parts of personal data that can identify an individual, so their identity can't be discovered without both parts of the data) in line with our retention guidelines.

Staff **must not**:

- Collect or process personal data for general or future use
- Collect unnecessary amounts of personal data
- Process personal data for any reason that is unrelated to their duties
- Delete or destroy (or attempt either) without the authority of their line manager and the Data protection manager.

Keeping personal data accurate

Where it's relevant to their duties, staff **must**:

- Check whether the personal data we receive is accurate and complete at the time it's collected
- Perform regular checks to ensure that the personal data we process remains necessary for the purpose we're holding it for, complete, accurate and up to date
- Tell their line manager and the Data Protection Manager of any change so it can be kept up to date

Data Protection Policy



- Where necessary or reasonable, amend inaccurate data or, with the prior consent of their line manager and the Data protection manager, securely destroy it.

In relation to their own personal data that we hold, staff **must**:

- Make sure it's accurate
- Tell us of any change so it can be kept up to date. We can't be held responsible for any errors unless they have notified us.
- If they believe that any of it should be destroyed or erased because it's no longer required or is inaccurate, inform their line manager and the Data protection manager.

Data access and accuracy

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

In addition, Community Matters will ensure that:

- It has a Data Protection Manager with specific responsibility for ensuring compliance with Data Protection
- Everyone processing personal information understands that they are contractually responsible for following good data protection practice
- Everyone processing personal information is appropriately trained to do so
- Everyone processing personal information is appropriately supervised
- Anybody wanting to make enquiries about handling personal information knows what to do
- It deals promptly and courteously with any enquiries about handling personal information
- It describes clearly how it handles personal information
- It will regularly review and audit the ways it holds, manages and uses personal information
- It regularly assesses and evaluates its methods and performance in relation to handling personal information
- All staff are aware that a breach of the rules and procedures identified in this policy may lead to disciplinary action being taken against them

Serious breaches will be reported to the Information Commissioner's Office (ICO) within 72 hours, and affected individuals will be informed where required.

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

Data Protection Policy



Keeping personal data safe

We must have appropriate security to prevent the personal data we hold being compromised. We'll take technical and organisational measures to ensure that personal data is protected, from the point of collection to the point of destruction, against any personal data breach.

We'll develop, implement and maintain safeguards that are appropriate to:

- The size and scope of our business and our available resources
- The amount of personal data that we process.

Our security measures include use of encryption technology and (where applicable) pseudonymisation (using artificial identifiers - or pseudonyms - to separately store parts of personal data that can identify an individual, so their identity can't be discovered without both parts of the data).

Our security procedures include:

- Only authorised personnel are permitted to access personal data:
- Personal data held in physical files must **not** be removed from their normal place of storage and electronic files must not be moved or destroyed, without the prior written consent of a director.
- Personal data stored on diskettes, CDs or other removable media must be kept in locked filing cabinets.
- Personal data held on a computer must be stored confidentially, be protected by at least one password and be encrypted or coded to prevent it being read if it's disclosed without authority.
- Desks and cupboards must be kept locked if they hold confidential information of any kind (personal data is always considered confidential).
- Paper documents must be shredded.
- Digital storage devices must be physically destroyed when they are no longer required.

We'll regularly evaluate and test the effectiveness of our security and have network back-up procedures to make sure that data on computers can't be accidentally lost or destroyed.

Staff **must**:

- Ensure all personal data is securely kept in a locked filing cabinet or password protected if computerised.
- Ensure workstation screens don't show personal data to passers-by and lock or log off of computers when they're left unattended.
- Follow all policies and procedures we put in place to maintain the security of all personal data from the point of collection to the point of destruction.
- Comply with and not attempt to avoid or evade the procedural, physical and technical safeguards we implement and maintain to protect the personal data.
- Be aware that those seeking information sometimes use deception to access it. Always

ask security questions to verify the identity of the individual and the legitimacy of the request, particularly before releasing personal data by telephone. If their identity cannot be verified, suggest that they put the request in writing.

- Get the prior written authority of their line manager or the manager in charge of the computer network before electronically transmitting personal data between locations (e.g. by email). A secure network must be in place (e.g. encrypted email).
- Forward to their line manager any request for personal data about another member of staff.
- Immediately inform their line manager if any stranger is seen in entry-controlled areas.

Staff **must not**:

- Disclose sensitive personal data to anyone other than the individual.
- Disclose an individual's confidential personal data to others (including the individual's family) without having first got the individual's clear and specific written statement of consent. An exception is if the person requesting has a need to know and is lawfully authorised to use the personal data.
- Print or make copies of the personal data without the prior written authority of their line manager. There must be a good business reason for printing or copying personal data. If authority is granted, the documents containing the personal data must be removed from the printer or photocopying machine as soon as they have been printed. This is particularly important in situations where the printer or photocopier is shared with other staff. Personal data copied or transferred to electronic storage devices (e.g. laptop, memory stick/card) must be securely encrypted.
- Transfer personal data to third parties without the prior written authority of their line manager, and the agreement of the third party to comply with our data security policies and procedures and to put satisfactory security measures in place.

Data storage

Information and records relating to service users will be stored securely and will only be accessible to authorised staff and volunteers. Internet security and security of all other tools, platforms and software will be monitored regularly to ensure any potential breach is identified early and measures taken to minimise any negative impact.

Community Matters will maintain a documented data retention schedule setting out how long each category of personal data will be retained. Data will be securely disposed of when no longer required.

Information will be stored for only as long as it is needed or required by statute and will be disposed of appropriately.

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

Processing sensitive personal data

Sensitive personal data is defined in the introduction to this policy. Before staff begin to process sensitive personal data, they **must** get the prior written consent of their line manager, telling them the reason for the processing and the types of sensitive personal data being processed. Sensitive personal data must **never** be processed without the knowledge of a line manager or a more senior manager in our business.

Processing sensitive personal data is not permitted unless we have a lawful basis for processing it and satisfy the limited circumstances set out below. This section sets out how an individual's data will be processed and the additional safeguards we have in place.

As an employer we're permitted to process our staff members' sensitive personal data if it's necessary to comply with employment laws. This includes statutes and regulations, regulatory requirements, case or common law and court orders. For example, to:

- Ensure staff members' health and welfare at work (e.g. compliance with working time regulations)
- Ensure staff work in a safe working environment
- Supply information on accidents to the Health and Safety Executive (e.g. accident records)
- Check staff members' immigration status for the right to work in the UK
- Avoid discriminating on the grounds of sex, race, disability, religion or belief, sexual orientation or age (e.g. processing equal opportunities monitoring forms)
- Maintain records of any statutory pay (e.g. sick, adoption, maternity, paternity, and shared parental)
- Process disciplinary and grievance records that may contain special categories of personal data
- Provide staff liability information under TUPE to a potential purchaser of our business.

We are also permitted to process individuals' special category data if it is in the substantial public interest. For example, this might be to:

- Prevent or detect an unlawful act, such as collecting data whilst monitoring for security purposes (e.g. where we need to protect property or money belonging to us, our customers or clients)
- Prevent fraud
- Disclose information where we suspect (in good faith) money laundering, terrorist financing or for the purposes of identifying terrorist property
- Determine if staff are eligible to join an occupational pension scheme, where we can't reasonably expect to get their consent and aren't aware they've withheld consent (we won't use the information to assess them or to make decisions about them)
- Identify or review equal opportunities or equal treatment (we'll only use particular types of special category data set out in the Act and will comply with its specific provisions on equal opportunity and treatment)

Data Protection Policy



- If necessary, protect the public against an individual's dishonesty, seriously improper conduct, unfitness or incompetence.

We may also process individuals' special category data where:

- We explain the reasons for needing it and then receive a very clear and specific written statement of consent (not just an action). This can be withdrawn at any time.
- They've already clearly made the information public (e.g. public social media posts)
- It's necessary to make or defend legal claims.
- They can't physically or legally give consent but the processing is necessary to protect a person's vital interests.

Additional safeguards

Information about how long we'll keep the personal data and when it's likely to be deleted is:

- For staff, at the end of this policy
- For other individuals, in the privacy notice and/or retention and erasure policy (if any) given to them.

We also confirm that:

- From the date processing begins up to 6 months after it ends, both documents will be maintained, reviewed and updated when necessary
- Both documents will be freely available to the ICO (if requested)
- We keep a record of our processing activities that sets out:
 - The lawful basis we are relying on
 - The condition relied on to process it
 - Whether the data is retained and deleted in accordance with our policy and, if not, why the policy hasn't been followed

Demonstrating compliance with all the principles

The GDPR requires us to effectively implement appropriate technical and organisational measures to ensure compliance with data protection principles. This means:

- We'll keep full and accurate records of all our data processing activities that:
 - are not occasional, or
 - could result in a risk to the rights and freedoms of individuals, or
 - involve the processing of sensitive personal data.

This may involve using guidance from the ICO.

We'll provide training to all staff who require it and regularly check our systems and processes to assess compliance with the GDPR. **Staff must:**

- Participate in all internal and external training

- Assist in checking our systems and processes when required.
- We'll approach all projects we undertake using our programs, computer systems or processes so that they account for privacy and data protection compliance from the start. We'll first conduct a data protection impact assessment, using guidance from the ICO.
- We'll make use of any other documentation that can show how we comply with the GDPR, such as:
 - This policy
 - Any data protection impact assessment reports
 - Any legitimate interest risk assessment reports
 - The location of personal data (where it is kept in paper file format)
 - Records of any consent obtained (**Staff must** keep evidence of any consent they obtain)
 - Any contracts we have with data processors
 - Information required for/contained in privacy notices
 - Information required for processing sensitive personal data.

Staff must comply with our procedures for demonstrating compliance the GDPR principles.

Transferring or sharing personal data with a third party

We won't transfer or share personal data with another person or organisation unless safeguards and written contractual arrangements are in place.

Data processors within the UK or the European Economic Area

Personal data must only be transferred to a data processor if:

- It's relevant to the services they provide, i.e. they need to know it,
- **Before any data is transferred** they agree in a written contract to:
 - Comply with our data security policies and procedures for personal data,
 - Put satisfactory security measures in place to comply with the GDPR, and
 - Ensure that any other data processor that they use to process the personal data is authorised by us and will do the same,
- It's been mentioned in the privacy notice provided to the individual who, if necessary, gave a clear and specific written statement of consent.

Disclosure

Community Matters may share data with other agencies such as the local authority, funding bodies and other voluntary agencies.

The Individual/Service User will be made aware in most circumstances how and with whom their information will be shared. There are circumstances where the law allows Community Matters to disclose data (including sensitive data) without the data subject's consent.

These are:

- Carrying out a legal duty or as authorised by the Secretary of State
- Protecting vital interests of an Individual/Service User or other person
- The Individual/Service User has already made the information public
- Conducting any legal proceedings, obtaining legal advice or defending any legal rights
- Monitoring for equal opportunities purposes – i.e. race, disability or religion
- Providing a confidential service where the Individual/Service User's consent cannot be obtained or where it is reasonable to proceed without consent: e.g. where we would wish to avoid forcing stressed or ill Individuals/Service Users to provide consent signatures.

Direct marketing

We may market our business to customers or clients and are required by law to protect their privacy. When sending marketing material to them by electronic means (e.g. text and email), we must comply with the GDPR and follow the ICO's guide to Privacy and Electronic Communications Regulations.

Individuals have a right to object to direct marketing and we must promptly adhere to any objection. Before staff plan to conduct direct marketing activities, they must consult with the Data protection manager.

Reporting a data protection breach

We will notify the ICO and sometimes individuals, where we are legally required to do so, if there has been a personal data breach.

If staff know or suspect that a personal data breach has occurred, they must:

- Not attempt to investigate the matter themselves
- Immediately contact their line manager and the Data protection manager
- Immediately take steps to protect all related evidence.

The rights of individuals

Individuals have the following rights:

- To withdraw consent at any time
- To be informed about how data is being collected and used by us

Data Protection Policy



- To request access to a copy of the personal data we hold (known as a 'data subject access request')
- To object:
 - to us processing personal data that has been justified on the basis of our legitimate interests or it being in the public interest
 - to decisions being taken by automated means
- To prevent us processing personal data for direct marketing purposes
- Subject to some exceptions:
 - to have any inaccurate data rectified, blocked, erased or (in some circumstances) destroyed
 - to have misleading data clarified and any incomplete data completed
 - to have personal data erased (known as 'the right to be forgotten')
 - to restrict or limit the way we use personal data
 - to have personal data moved, copied or transferred from one IT environment to another.

A request can be made to any person in the business, verbally or in writing. If staff receive one of the above requests, **they must:**

- Record and keep the details, particularly for requests made by telephone or in person, and check with the person making the request that they've accurately recorded it (to avoid later disputes)
- Immediately forward the request to their line manager and the Data Protection manager

Comply with any procedures we have to respond to a request. In addition to the above rights, individuals have a right:

- To be notified if their personal data has been breached if it's likely to result in a high risk to their rights and freedoms
- Complain to the ICO
- Claim compensation for damages caused by breaching the Act or the GDPR.

Procedures involving staff rights

To make a request in relation to one of the rights listed above, staff should apply to the Data protection manager. Ideally this should be in writing, to avoid unnecessary delays.

No fee is required to exercise these rights unless the request is clearly unfounded, excessive or repetitive. In those circumstances, we reserve the right to either charge a fee based on our administrative costs of dealing with their request or to refuse to respond to it.

We may need to request more information from the staff member to help us confirm their identity, to avoid disclosing their personal data to anyone else who shouldn't receive it.

Data Protection Policy



Otherwise, we'll usually respond to staff requests within one month of the day after we received the request. We may extend the time to comply by a further 2 months if the request is complex or if we receive a number of them from the staff member.

If staff want to complain that these rules aren't being followed, they should raise the matter with the Data protection manager. If the matter isn't resolved to the staff member's satisfaction, it may then be raised as a formal grievance under our grievance procedure.

Right to information about decision making

Where we've processed personal data about an individual, and the results produced by the processing are applied to them, they can request us to provide the underlying reason for the processing and express their point of view to contest the decision.

If we receive such a request, we must comply as soon as possible and within one month of receiving it.

Right to object to processing

An individual can tell us not to:

- Process their personal data
- Process their personal data for the specified reason or in the specified manner we've informed them of, if that processing causes an unwarranted interference with their rights.

If the individual does this, we must, within one month (beginning with the date we receive their instruction) state:

- That we've complied, or intend to comply, or
- Why we haven't complied, or won't, or
- What part of their instruction we've complied with, or will comply with, and why we won't comply with the rest of it.

We won't have to comply until we've received more information about the individual's identity or to locate the data that the instruction relates to. We will only do this where we:

- Reasonably require the information, and
- Have informed them of this.

Monitoring of staff

Monitoring of our communication equipment is covered in Community Matters' **Communication Policy**.

Reporting a breach of this policy

Line managers will usually deal with concerns and disciplinary issues about the misuse of personal data or other breaches of this policy.

Data Protection Policy



Staff should report breaches of this policy to their line manager and the Data protection manager.

Staff won't be penalised for reporting a breach of this policy in good faith, even if it's mistaken. We'll support staff against detrimental treatment or recrimination.

The identity of staff will be protected if requested and it's reasonably possible to achieve.

Consequences of breaching this policy

The provisions of this policy will be rigorously enforced. Any breach of this policy will result in a disciplinary investigation.

Employees: We'll carry out disciplinary investigations using our disciplinary procedures. In certain circumstances they may be summarily dismissed for gross misconduct.

Self-employed or unpaid staff (i.e. volunteers and people on work experience): We won't use our disciplinary procedures - or any other modified procedure based on it - to take any necessary disciplinary action against them.

Depending on the outcome of the investigation and the seriousness of the breach, we may (for self-employed staff) cancel their contract with us or (for staff who are volunteers or on work experience) remove them from our workforce.

Staff working for us in any other capacity: Any necessary disciplinary action we take against them will be subject to a similar, but modified version of our disciplinary procedures. Depending on how they work for us, they may not be entitled to:

- A meeting (their line manager will let them know if a meeting is needed)
- Have the stages in the procedure concluded within the timeframes mentioned in our disciplinary procedures
- Bring a companion with them (their line manager will let them know if they can)
- Appeal our decision.

Depending on the outcome of the investigation and the seriousness of the offence, we may:

- (If they're a director, officer or worker) take informal or formal disciplinary action against them
- (If they're a worker, paid intern, trainee or apprentice) cancel their contract with us
- (If they're an agency worker) remove them from our workforce.

Staff could be criminally liable if they knowingly or recklessly disclose personal data in breach of the Act or the GDPR.

Keeping the personal data we hold

We'll keep individuals' personal data for no longer than is necessary for the purpose it was obtained for.

To determine the appropriate retention period for personal data, we consider:

- The amount, nature and sensitivity of it
- The potential risk of harm from unauthorised use or disclosure of it
- The reasons why we process it and whether we can achieve that through other means.

Staff **must** comply with our retention guidelines when processing data for us and, when a retention period expires, notify their line manager and the Data protection manager.

If the data is to be destroyed then, as a general rule, paper material should be shredded and any hard disks or other storage devices used to store electronic documents should be physically destroyed.

The Data Protection Manager can give further guidance about how to destroy personal data.

Keeping the personal data we hold on staff

We'll usually keep staff members' personal data while they remain working for us.

Once the staff member is no longer working for us, we determine the appropriate retention period for their personal data by considering the above factors. We'll also consider:

- The effect of employment legislation and other legal obligations that set out minimum periods for keeping personal data
- The risk of having to rely on it in a tribunal, County Court or High Court claim.

To protect us against such risks, we take the view that staff members' personal data should be kept beyond the time limit that applies for making a claim against us. We'll therefore usually apply the minimum periods for keeping personal data as set by law and the time limit that applies for making any tribunal or court claims laws against us, and then add a further year. This is because claims can be issued after the time limit passes if claimants get an extension or if there is a delay before any claim reaches us. In some circumstances longer periods may be appropriate.

See below for full details of the retention periods for personal data after a staff member stops working for us. Thereafter, their personal data will be securely destroyed (unless we are subsequently subject to other legal obligations to retain it for a longer period).

Retention periods for personal data we hold on staff	
Type of record/document	Recruitment records transferred to a personnel file May include: • Notes from interviews and short-listing exercises • Pre-employment verification details E.g. qualifications, reference • Criminal records checks • Health questionnaire or medical report
Reason held	If required for the ongoing working relationship
Minimum retention period usually required	While staff are working for us and 6 years after employment ends
Recommended retention period	While staff are working for us and 7 years after employment ends
Reason for recommended retention period	Extra year to allow for any claims that may be issued Allows for situations where the legal time limit to make a claim is extended by a court/tribunal and/or where there's been a delay before we receive a claim

Type of record/document	Personnel records May include details/records of: • Annual leave • Absence • Annual appraisals/performance reviews • Disciplinary investigations and hearing outcomes • Performance/capability investigations and hearing outcomes • Grievances, investigations and meeting outcomes • Consents for the processing of special category data • Resignation, termination and retirement
Reason held	So we can comply with our employment and other legal obligations
Minimum retention period usually required	While staff are working for us and 6 years after employment ends
Recommended retention period	While staff are working for us and 7 years after employment ends
Reason for recommended retention period	Extra year to allow for any claims that may be issued Allows for situations where the legal time limit to make a claim is extended by a court/tribunal and/or where there's been a delay before we receive a claim

Data Protection Policy



Type of record/document	Employment or other contracts and any agreements with unpaid staff Includes: • Contracts of employment with employees, workers (including casual workers) • Agreements with contractors • Written particulars of employment • Documented changes to terms and conditions
Reason held	As a record of the obligations of the parties whilst employed with us
Minimum retention period usually required	While staff are working for us and 6 years after employment ends
Recommended retention period	While staff are working for us and 7 years after employment ends
Reason for recommended retention period	Extra year to allow for any claims that may be issued Allows for situations where the legal time limit to make a claim is extended by a court/tribunal and/or where there's been a delay before we receive a claim

Type of record/document	PAYE records
Reason held	Statutory requirement
Minimum retention period usually required	3 years after the end of the tax year to which they relate
Recommended retention period	Minimum of 7 years after employment ends
Reason for recommended retention period	Extra years to allow for any contractual pay claims that may be issued Allows for situations where the legal time limit to make a claim is extended by a court/tribunal and/or where there's been a delay before we receive a claim

Data Protection Policy



Type of record/document	Payroll and wage records for companies Includes records of: • Overtime • Bonuses • Expenses • Benefits in kind
Reason held	Statutory requirement
Minimum retention period usually required	6 years from the financial year-end in which payments were made
Recommended retention period	7 years after employment ends
Reason for recommended retention period	Extra years to allow for any contractual pay claims that may be issued Allows for situations where the legal time limit to make a claim is extended by a court/tribunal and/or where there's been a delay before we receive a claim

Type of record/document	Bank details
Reason held	To comply with contractual obligations to pay salary, overtime, expenses or bonuses
Minimum retention period usually required	None
Recommended retention period	To be deleted as soon as possible after staff are no longer employed by us (or unpaid staff no longer work for us) and final payments have been made
Reason for recommended retention period	To avoid holding unnecessary personal data

Data Protection Policy

A red circular logo with the text "COMMUNITY MATTERS" in white, uppercase letters.

COMMUNITY
MATTERS

Type of record/document	Immigration checks
Reason held	Statutory requirement to comply with right-to-work laws
Minimum retention period usually required	2 years after employment ends
Recommended retention period	3 years after employment ends
Reason for recommended retention period	Extra year to allow for any claims made against us Allows for situations where the legal time limit to make a claim is extended by a court/tribunal and/or where there's been a delay before we receive a claim

Type of record/document	Records required by the Working Time Regulations recording staff opting out of the 48-hour week
Reason held	Statutory requirement
Minimum retention period usually required	2 years from the date they opted out
Recommended retention period	3 years from the date they opted out
Reason for recommended retention period	Extra year to allow for any claims made against us Allows for situations where the legal time limit to make a claim is extended by a court/tribunal and/or where there's been a delay before we receive a claim

Type of record/document	Records required by the Working Time Regulations proving compliance with it Includes records of: • Timesheets for workers who haven't opted out of the 48-hour week, young workers, night workers • Health assessment records for all night workers
Reason held	Statutory requirement
Minimum retention period usually required	2 years from the date they were made
Recommended retention period	3 years from the date they were made
Reason for recommended retention period	Extra year to allow for any claims made against us Allows for situations where the legal time limit to make a claim is extended by a court/tribunal and/or where there's been a delay before we receive a claim

Data Protection Policy



Type of record/document	Records required by the Minimum Wage Act such as: Recording hours worked and payments made to workers to prove compliance
Reason held	Statutory requirement
Minimum retention period usually required	3 years after the end of the pay reference period following the one that the records cover e.g. Salary paid each calendar month: May 2018 records must be kept until 1 July 2021
Recommended retention period	Minimum of 7 years after employment ends
Reason for recommended retention period	Extra years to allow for any contractual pay claims that may be issued Allows for situations where the legal time limit to make a claim is extended by a court/tribunal and/or where there's been a delay before we receive a claim

Type of record/document	Maternity documentation: - Maternity payments - Maternity leave dates - Period without maternity payment - Maternity certificates/MAT B1 showing expected week of childbirth
Reason held	Statutory requirement
Minimum retention period usually required	3 years after the end of the tax year in which the maternity pay period ends
Recommended retention period	4 years after the end of the tax year in which the maternity pay period ends
Reason for recommended retention period	Extra year to allow for any claims made against us Allows for situations where the legal time limit to make a claim is extended by a court/tribunal and/or where there's been a delay before we receive a claim

Data Protection Policy



Type of record/document	Records required by the Injuries, Diseases and Dangerous Occurrences Regulations such as: Accident reports for any reportable accident, death or injury in connection with work
Reason held	Statutory requirement
Minimum retention period usually required	At least 3 years from the report date
Recommended retention period	At least 4 years from the report date
Reason for recommended retention period	Extra year to allow for any claims made against us Allows for situations where the legal time limit to make a claim is extended by a court/tribunal and/or where there's been a delay before we receive a claim

Type of record/document	Collective agreements
Reason held	To record our agreements with trade unions and the workforce
Minimum retention period usually required	While staff are working for us and 6 years after employment ends
Recommended retention period	While staff are working for us and 7 years after employment ends
Reason for recommended retention period	Extra year to allow for any claims made against us Allows for situations where the legal time limit to make a claim is extended by a court/tribunal and/or where there's been a delay before we receive a claim

Data Protection Policy



Type of record/document	Records relating to travel including: • Where they have stayed • Payments made • Any foreign country safety assessments • Season ticket loans or other such advances
Reason held	For monitoring compliance with employment obligations regarding travel and repayment of any loans
Minimum retention period usually required	While staff are working for us and 6 years after employment ends
Recommended retention period	While staff are working for us and 7 years after employment ends
Reason for recommended retention period	Extra year to allow for any claims made against us Allows for situations where the legal time limit to make a claim is extended by a court/tribunal and/or where there's been a delay before we receive a claim