



Scargill Movement

Privacy Notice for Members/Applicants & Working Friends/Applicants

The Scargill Movement (Community) is committed to maintaining the accuracy, confidentiality and security of your personal information. This Privacy Notice describes the personal information that we collect from or about you, how we use it and to whom we disclose that information.

What Personal Information Do We Collect?

For the purposes of this Privacy Notice, personal information is any information about an identifiable individual. Personal information does not include anonymous or non-personal information.

We collect and maintain different types of personal information in respect of those individuals who seek to be, are, or were members of the Community (employed by us), and for those who seek to be, are or were Working Friends, including the personal information contained in:

- CVs and applications;
- references and interview notes;
- DBS and vetting information;
- Education and training information;
- Right to work information;
- Photographs, testimonials, video and audio recordings including CCTV imagery;
- letters of offer and acceptance of employment and other employment records;
- policy acknowledgement sign-off sheets;
- payroll information; including but not limited to national insurance number, banking and deposit information and national insurance number;
- wage and benefit information including annual leave information;
- forms relating to the application for welfare benefits;
- Health questionnaires and risk assessments including details of any medical condition or medication you are taking;
- beneficiary and emergency contact information;
- Disciplinary and grievance records;
- Your driving licence and insurance documentation; and
- Equal opportunities monitoring forms

In addition to the examples listed above, the personal information we collect includes information such as your name, home address, telephone, personal email address, date of birth, employee identification number, ethnicity, marital status, nationality, next of kin/emergency contact information, salary and any other information necessary for the day to day running of the Community, which is voluntarily disclosed in the course of a member's application for and membership (employment) with us, or in the course of a Working Friend's application for that status with us.

The above lists are non-exhaustive and applies across the Community & Working Friends.

As a general rule, we collect personal information directly from you. In most circumstances where the personal information that we collect about you is held by a third party, we will only process it in accordance with our legitimate interests, where necessary for the performance of our contracts or where obligated by law. We will take reasonable steps to ensure that such third parties have represented to us that they have the right to disclose your personal information to us. This is likely to be limited to references and background checks (DBS).

Where permitted or required by applicable law or regulatory requirements, we may collect information about you without your knowledge or consent.

Why Do We Collect Personal Information?

The personal information collected is used and disclosed for our business purposes, including establishing, managing or terminating the membership (employment), Working Friend relationship and complying with our obligations to you. It is necessary for the performance of our contract/agreement with you and/or performing our obligations under a contract/agreement as well as to meet our legal obligations and legitimate interests. In respect of special category data, which includes health data, it is necessary for your employment, social security and social protection, reasons of substantial public interest and/or for reasons of public interest in the area of public health, such as protecting against serious threats to health. Such uses include:

- determining eligibility and suitability for initial employment, work as a volunteer, including profiling from any previous job application to us, right to work checks and the verification of references and qualifications;
- administering pay and benefits including holiday pay;
- processing employee work-related claims (e.g. insurance claims, etc.)
- establishing training and/or development requirements;
- conducting performance reviews and determining performance requirements;
- assessing qualifications and suitability for a particular job, task or promotion;
- gathering evidence further to the disciplinary, grievance or whistleblowing procedure;
- establishing a contact point in the event of an emergency (such as next of kin);
- considering, assessing and preventing inequality or health & safety incidents or risks;
- for pandemic monitoring and infection control purposes;
- complying with all regulatory and legislative requirements;
- compiling contact lists for internal purposes only;
- analysing workforce trends e.g. impact of Covid-19 or other pandemics or regulatory or legislative changes;
- ensuring your security and the security of Community held information and data; and
- such other purposes as are reasonably required by us for the performance of your contract; to protect vital interests; for the performance of a task in the public interest; to comply with our legal obligations; in accordance with our legitimate business interests or for the purpose of assessing your working capacity.

Monitoring

The work output of members/volunteers, whether in paper record, computer files, or in any other storage format belongs to us, and that work output, and the tools used to generate that work output, are always subject to review and monitoring by us.

In the course of conducting our business, we may monitor member/volunteer activities, attendance and our premises and property. Where in use, CCTV cameras are there for the protection of members/volunteers and third parties, to protect against theft, vandalism and damage to our goods and property and for quality control purposes. Generally, recorded images are routinely destroyed and not shared with third parties unless there is suspicion of a crime, in which case they may be turned over to the police or other appropriate government

agency or authority. Members/volunteers are referred to our CCTV Policy for further information. Pursuant to our Monitoring of Business Communications Policy and Procedure and our Computer, Email and Internet Usage Policy (see Data Protection Policy).

This section is not meant to suggest that all members/volunteers will in fact be monitored or their actions subject to constant surveillance. It is meant to bring to your attention the fact that such monitoring may occur and may result in the collection of personal information from members/volunteers (e.g. through their use of our resources). When using Community equipment or resources members/volunteers should not have any expectation of privacy with respect to their use of such equipment or resources.

How Do We Use Your Personal Information?

We may use your personal information for the purposes described in this Policy, or for any additional purposes that we advise you of and where your consent is required by law we have obtained your consent in respect of the use or disclosure of your personal information.

We may use your personal information without your knowledge or consent where we are permitted or required by applicable law or regulatory requirements to do so.

When Do We Disclose Your Personal Information?

We may share your personal information with our members, contractors, advisers or consultants and other parties who require such information to assist us with establishing, managing, funding or terminating our employment relationship with you, including: professional advisers, parties that provide products or services to us or on our behalf and parties that collaborate with us in the provision of products or services to you.

Also, your personal information may be disclosed:

- as necessary for the performance of our contract/agreement with you
- as permitted or required by applicable law or regulatory requirements. In such a case, we will try to not disclose more personal information than is required under the circumstances;
- to comply with valid legal processes such as warrants or court orders;
- as part of our regular reporting activities, i.e. if necessary for the performance of your contract, to comply with a legal obligation or as part of our legitimate business interests;
- to protect the rights and property of Scargill Movement or others;
- during emergency situations or where necessary to protect the vital interests or safety of a person or community of persons;
- to assess your working capacity;
- if in the substantial public interest;
- where the personal information is publicly available; or
- with your consent.

Notification and Consent

Privacy laws do not generally require us to obtain your consent for the collection, use or disclosure of personal information for the purpose of establishing, managing or terminating the employment/agreement relationship. In addition, we may collect, use or disclose your personal information without your knowledge or consent where we are permitted or required by applicable law or regulatory requirements to do so.

Where your consent was obtained or required for our collection, use or disclosure of your personal information, you may, at any time, subject to legal or contractual restrictions and reasonable notice, withdraw your consent. All communications with respect to such withdrawal or variation of consent should be in writing and addressed to the Data Protection Lead.

How is Your Personal Information Protected?

We endeavour to maintain physical, technical and procedural safeguards that are appropriate to the sensitivity of the personal information in question. This includes the use of firewalls and encryption as well as other information security requirements, systems and procedures. These safeguards are designed to protect your personal information from loss and unauthorised access, copying, use, modification or disclosure.

We also use data sharing agreements, data processing agreements and the standard contractual clauses to protect your data where it is being shared, processed and/or transferred to a third party.

How Long is Your Personal Information Retained?

For unsuccessful applicants or those who do not accept a position with us, we will generally destroy your data after 6 months unless you have requested that we retain it for longer.

For recruited members (employees), Working Friends, except as otherwise permitted or required by applicable law or regulatory requirements, we will only retain your personal information for as long as we believe it is necessary to fulfil the purposes for which the personal information was collected (including, for the purpose of meeting any contractual, legal, accounting or other reporting and regulatory requirements or obligations). We may, instead of destroying or erasing your personal information, make it anonymous such that it cannot be associated with or tracked back to you. In most cases your data will be deleted 6 years after you have left the community or as otherwise set out in accordance with our data retention schedule and/or as required by law. A safeguarding summary of name, time on community, and working teams will be kept for 75 years in line with our safeguarding policy. There may be other reasons our safeguarding policy requires us to keep your personal information for a longer period.

Updating Your Personal Information

It is important that the information contained in our records is both accurate and current. If your personal information happens to change during the course of your membership/active volunteership, please keep us informed of such changes.

In some circumstances we may not agree with your request to change your personal information and will instead append an alternative text to the record in question.

Access to Your Personal Information

You can ask to see the personal information that we hold about you. If you want to review, verify or correct your personal information, please contact the Data Protection Lead. Please note that we ask that any such communication be in writing.

When requesting access to your personal information, please note that we may request specific information from you to enable us to confirm your identity and right to access, and to assist us in searching for and provide you with the personal information that we hold about you. In specific circumstances, we may charge you a fee to access your personal information however we will advise you if this is the case and of any fee in advance.

Your right to access the personal information that we hold about you is not absolute. There are instances where applicable law or regulatory requirements allow or require us to refuse to provide some or all of the personal information that we hold about you. In addition, the personal information may have been destroyed, erased or made anonymous in accordance with our record retention obligations and practices.

If we cannot provide you with access to your personal information, we will inform you of the reasons why, subject to any legal or regulatory restrictions.

Your other legal rights

Data protection legislation also provides you with certain other rights. These are not always absolute rights and must be considered in the wider scope of the legislation. These rights are:

- right to erasure, also known as the right to be forgotten. The broad principle underpinning this right is to enable an individual to request the deletion or removal of personal data where there is no compelling reason for its continued processing. In some circumstances this is not an absolute right;
- right to restrict processing. You have the right to 'block' or suppress processing of personal data. Again, this is not an absolute right and will depend on the circumstances and any other legal/statutory obligations we may have;
- right to data portability – this is the right to have information provided in a structured, commonly used machine-readable format;
- right to object to processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling);
- rights related to automated decision making including profiling.