People and Workforce Development

Our core data protection obligations and commitments are set out in the Council's Corporate Privacy Notice on our website at Data Protection – Privacy Notice.

This notice provides additional privacy information for the following service areas:-

- Workforce and Partnerships;
- HR Operations and Strategy; and
- Payments, Systems and Registrars.

It provides information for:-

- Applicants;
- Employees (and former employees);
- Workers (including agency, casual and contracted staff); volunteers; and
- Trainees and those carrying out work experience.

It describes how we collect, use and share personal information about you:-

- Before, during and after your working relationship with us ends; and
- The types of personal information we need to process, including information the law describes as 'special' because of its sensitivity.

Purpose(s) of processing data

The Council collects and processes personal and sensitive personal data relating to its employees in order to manage the employment relationship.

The main purposes for processing your personal information are:-

- Undertaking pre-employment and verification checks during the recruitment process;
- In the recruitment decision-making process including internal recruitment;
- Determining/reviewing the terms on which you work for us;
- Checking you are legally entitled to work in the UK;
- Paying you and, if you are an employee, deducting tax and national insurance contributions;
- Processing and liaising with your pension provider;
- Administering the contract that we have entered into with you;
- Maintaining accurate and up to date employment records and contact details;
- Business management and planning including accounting and auditing;
- Conducting performance reviews, managing performance and determining performance requirements;
- Making decisions about salary reviews and compensation;
- Assessing qualifications for a particular job or task, including decisions about promotion;
- Gathering evidence for possible grievance, capability, sickness absence management or disciplinary hearings;
- To operate and keep records of:
    - Disciplinary and grievance process;
    - Employee performance and related processes;;
    - Education, training and development requirements
    - Absence and absence management procedures; and
    - All types of leave.
- Making decisions about your continued employment or engagement;
- Making arrangements for the termination of our working relationship;

- Dealing with legal disputes involving you, or other employees, workers and contractors, including accidents at work;
- Ascertaining your fitness to work;
- Managing sickness absence;
- Complying with health and safety obligations and public access legislation
- To prevent fraud, including sharing and matching of personal information for the national fraud initiative;
- To conduct data analytics studies to review and better understand employee retention and turnover rates;
- For equal opportunities and monitoring purposes;
- To monitor staff engagement and survey results; and
- To offer you work-related benefits and support and networking opportunities.

Personal Data

In order to carry out activities and obligations as an employer we process personal information in relation to:-

- Personal contact details such as name, title, addresses, telephone numbers, and personal email addresses;
- Personal demographics (including date of birth, gender, marital status, civil partnerships and caring responsibilities);
- Contact details such as names, addresses, personal e-mail address, telephone numbers next of kin and emergency contact(s);
- Recruitment records (including CV, application form, references, pre-employment and verification checks e.g. copy of qualifications, driving licence, passport);
- Employment records (including your workplace, start date, job title, national insurance number, training records, reviews, professional memberships, proof of eligibility to work in the UK and security checks);
- Bank account details, payroll records and tax/national insurance status information;
- Salary, annual leave, pension and benefits information;
- Statutory deduction information such as student loans and court orders;
- Disciplinary and grievance information;
- Photographs, CCTV footage and other information obtained through electronic means;
- Information about your use of our information and communications systems;
- Staff survey responses and results; and
- Health and Safety information such as accident and incident reporting.

Special Category Data

We may also collect, store and use the following "special categories" of more sensitive personal information:

- Trade union membership (including complying with employment law and paying subscriptions);
- Information about your race or ethnicity, religious beliefs, sexual orientation and political opinions (including ensuring meaningful equal opportunities monitoring and reporting but only where you have opted to provide this data as part of your application for employment);
- Medical information including physical health or mental condition, sickness and occupational health records (including to comply with employment and other laws, ensure health and safety, assess fitness to work and monitor and manage absence); and
- Offences (including alleged offences), criminal proceedings, outcomes and sentences.

These special categories or sensitive personal information require higher levels of protection. We need to have further justification for collecting, storing and using this type of personal information. We process special categories of personal information, which is used in the following circumstances:

- With your explicit written consent;
- To meet our legal and/or statutory obligations;
- Where it is needed in the public interest (including equal opportunities monitoring in relation to the occupational pension scheme);
- Where it is needed to assess your working capacity on health grounds;
- Where it is needed in relation to a legal claim; and
- Where it is needed to protect your interests and you are not capable of giving consent.

You should be aware that it is not a condition of your contract with us that you agree to any request for consent from us and that where consent is given, you have the right to withdraw it at any time (without affecting the lawfulness of our processing prior to the withdrawal of your consent).

We recognise the need to treat staff personal data in a fair and lawful manner and aim to maintain high standards and adopt best practice for our record keeping. Your information is never collected or sold for direct marketing purposes.

We will only collect information about criminal convictions if it is appropriate for the employment role and where we are legally permitted or required to do so. We collect information about criminal convictions as part of the recruitment process or may be notified of information directly by you or a third party in the course of your recruitment or employment.

Legal basis for processing

The legal conditions we rely on for processing your personal information are set out in Articles 6(1) (b), (c), (e) and 6(f) and Articles 9 (2) (b), (f) and (h) of the General Data Protection Regulations (GDPR) and are listed below:

- Entering into or performing obligations under your contract of employment
- Performing or exercising obligations or rights under employment law, social security law or social protection;
- General legal obligations we must meet;
- Where it is needed to assess your working capacity on health grounds, subject to appropriate confidentiality safeguards;
- Where it is needed in relation to exercising or defending legal rights (e.g. in relation to legal proceedings and claims);
- Your consent (in situations where you have a genuine choice and control over whether your information is processed, including the right to withdraw your consent at any time without detriment);
- Our legitimate interests (or those of a third party) provided your interests and fundamental rights do not override those interests;
- Fraud prevention and protection of public funds;
- Compliance with any Court Orders; and
- Where it is needed to protect your interests (or someone else's interests) and you are not capable of giving your consent.

Examples of our legitimate interests are:

- To monitor your use of our information and communication systems to ensure compliance with our IT policies; and

- To ensure network and information security, including preventing unauthorised access to our computer and electronic communications systems and preventing malicious software distribution.

Consequences if statutory or contractual information is not provided

If you fail to provide certain information when requested, we may not be able to perform the contract we have entered into with you (such as paying you or providing a benefit), or we may be prevented from complying with our legal obligations (such as to ensure the health and safety of our workers).

This could also damage the employment relationship /result in breach of contract.

Information sharing

Your information will be shared internally within the People and Workforce Development service area. Personal data and employment data will be shared with your line manager and managers in the service area in which you work.

Additionally we may share your information as follows:-

- We may share information about you with third parties where required by law, where necessary to fulfil your contract of employment or where we or a third party has a legitimate interest;
- For the purposes of the National Fraud Initiative conducted by central government under Section 33 and Schedule 9 of the Local Audit and Accountability Act 2014;
- In connection with school workforce census as provided for in Section 114 of the Education Act 2005 and the associated Education (Supply of Information about the School Workforce) (No.2) (England) Regulations 2007/2260, which affects some directly employed council staff working in education;
- To obtain pre-employment references from other employers;
- To obtain necessary criminal record checks from the Disclosure and Barring Service;
- Under our duties to comply with any court orders that may be imposed;
- To offer you work-related benefits and to protect you at work; and
- To enable you to pay union subscriptions directly from your salary.

Any disclosures of personal data is always made on a case-by-case basis, using the minimum personal data necessary for the specific purpose and circumstances and with the appropriate due diligence undertaken and security controls in place.

Where we get our Information

As well as information directly collected from candidates in the recruitment process and from employees during the course of employment, we also collect or receive information from:-

- Former employers;
- Referees;
- Employment agencies;
- Disclosure and Barring Service;
- Complainants (e.g. service users/employees);
- Next of kin;
- Health professionals;
- Public sources, if relevant to employment and job role; and
- Government departments and agencies.

Information is only obtained from these third parties where is it necessary for the fulfilment of your contract, including your ability or otherwise to perform your contractual obligations and to support you to do so under the terms of your employment.

Data Retention Criteria

We will only retain your personal information for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any future legal, accounting, or reporting requirements.

Once your employment ends we must continue to retain necessary information in accordance with our corporate records management policy to fulfil legal, statutory, regulatory and pension requirements.

Data Transfers beyond European Economic Area

We do not transfer any of your personal information outside the European Economic Area ('EEA').

Your rights

Information about exercising your rights can be found on the council's website Exercising Your Individual Rights.

Security

We use appropriate technical, organisational and administrative security measures to protect any information we hold in our records from loss, misuse, and unauthorised access, disclosure, alteration and destruction. We have written procedures and policies, which are regularly audited, and the audits are reviewed at senior level.

Data Protection Officer

You can contact the Council's Data Protection Officer at information.governance@tameside.gov.uk or by calling 0161 342 8355.

Automated Decisions

No automated decisions are made throughout this process.

Updates

We may update or revise this Privacy Notice at any time so please refer to the version published on our website for the most up to date details on our Data Protection page/