Data Controller – Dover District Council, White Cliffs Business Park, Whitfield, Dover CT16 3PJ

Data Protection Officer – Joe Couchman, Dover District Council, White Cliffs Business Park, Whitfield, Dover CT16 3PJ
Email: data.protection@dover.gov.uk Tel: 01304 872318

Employee Privacy Notice

Processing activity

Dover District Council is committed to protecting the privacy and security of your personal information. This privacy notice describes how we collect and process personal information about you during and after your employment at the Council.

This privacy notice tells you what to expect when we collect personal information about you. It applies to all employees, ex-employees, agency staff, contractors, interns and secondees. However, the information we will process about you will vary depending on your specific role and personal circumstances.

We will only use your personal information for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to use your personal information for an unrelated or new purpose, we will update this privacy notice to explain the new purpose and the legal basis that permits us to do so.

Where appropriate, we will also provide 'just-in-time' notices to inform you of any additional processing not covered in this notice. Please note that in certain circumstances, we may process your personal information without your knowledge or consent, but only where this is required or permitted by law.

This privacy notice does not form part of any contract of employment or other contract to provide services.

Information requirements - we process personal information relating to:

1. **Your employment** - we use the following information to carry out the contract we have with you, provide you access to business services required for your role and manage our human resources processes:

- personal contact details such as your name, address, contact telephone numbers (landline and mobile) and personal email addresses;
- your date of birth, gender and NI number;
- a copy of your passport or similar photographic identification and / or proof of address documents
- Documents relating to driving license/status
- marital status;
- next of kin, emergency contacts and their contact information;
- employment and education history including your qualifications, job application, employment references, right to work information and details of any criminal convictions that you declare;
- location of employment;
- details of any secondary employment, political declarations, conflict of interest declarations or gift declarations;
- disclosure barring service checks according to your job;
- any criminal convictions that you declare to us;
- your responses to staff surveys if this data is not anonymised;
- your political declaration form in line with our policy and procedure regarding party political activities;
- evidence of your right to work in the UK/immigration status.

2. **Salary, pension and expenses** - we process this information for the payment of salaries, pensions and other employment related benefits for our staff. We also process information for the administration of statutory and contractual leave entitlements such as holiday or maternity leave:

- information about your job role and your employment contract including; your start and leave dates, salary (including grade and salary band), any changes to your employment contract, working pattern (including any requests for flexible working)
- details of your time spent working and any overtime, expenses or other payments claimed.
- details of any leave including sick leave, holidays, special leave etc.
- pension details including membership of both state and occupational pension schemes (current and previous)
- your bank account details, payroll records and tax status information
- Trade Union membership for the purpose of the deduction of subscriptions directly from salary
- details relating to maternity, paternity, shared parental and adoption leave and pay. This includes forms applying for the relevant leave any relevant documentation relating to the nature of the leave you will be taking
- details of vehicles driven by you and destinations (for mileage claims)
- details of expenses incurred by you in the performance of your job which include places where expenditure was incurred
- details about your physical form e.g. clothing sizes for the purposes of council provided workwear.

3. **Performance and training -** we use this information to assess your performance, to conduct pay and grading reviews and to deal with any employer/employee related disputes. We also use it to meet the training and development needs required for your role:

- information relating to your performance at work e.g. probation reviews, appraisals, performance development reviews, promotions
- grievance and dignity at work matters and investigations to which you may be a party or witness
- disciplinary records and documentation related to any investigations, hearings and warnings/penalties issued
- whistleblowing concerns raised by you, or to which you may be a party or witness
- information related to your training history and development needs

4. **Health and wellbeing and other special category data** - we use the following information to comply with our legal obligations and for equal opportunities monitoring. We also use it to ensure the health, safety and wellbeing of our employees:

- health and wellbeing information either declared by you or obtained from health checks, eye examinations, occupational health referrals and reports, sick leave forms, health management questionnaires or fit notes i.e. Statement of Fitness for Work from your GP or hospital
- accident records if you have an accident at work
- details of any desk audits, access needs or reasonable adjustments
- information you have provided regarding protected characteristics as defined by the Equality Act 2010 for the purpose of equal opportunities monitoring - includes racial or ethnic origin, religious beliefs, disability status, and gender identification and may be extended to include other protected characteristics
- information about criminal convictions/allegations and offences

5. **Compliance with corporate policies etc., security of our premises & electronic communications' systems** – we have implemented industry standard security measures to assist us to keep our systems and premises secure. These security measures are primarily focused on ensuring we can detect, block and respond to malicious software (malware) and intrusion attempts and to ensure we keep our business data and your personal data secure and confidential. The security measures implemented include:

- **system security** – automated scanning of incoming and outgoing emails, workstations, applications and our networks for potential threats. Threats, such as phishing emails, data leakage, presence of malware, noncompliance with our policies, or other unusual activity will be escalated to our ICT and Security team for review and response;

- **logs and audit trails** – logging and audit trail capabilities on all systems accessed by you (for example, passwords, physical access logs, system and transactional logs from applications, systems and communication channels etc.). We have implemented automated tools to record and monitor information about your usage of login credentials, access to applications and websites and other activities carried out by you while using our systems. The automated tools have been configured to protect confidential information (including personal data) and to ensure our systems are protected against malware and other threats. These tools will also alert our ICT and Security team of such threats and of any potential non-compliance with our policies. Given most of web traffic over our systems is encrypted, the automated tools that monitor for malware and data leakage may also decrypt this traffic to ensure the continued effectiveness of these controls. Additionally, activities of users who have privileged access to our systems might be subject to a higher level of monitoring by automated tools, given higher potential business impact in case of compromise/misuse of such credentials. From time to time, we may also share the audit logs containing information about the activities performed by users on our systems in order to investigate any system issues or data breaches;

- **CCTV** – we operate CCTV to help keep our premises secure. Images of you may be captured as part of the CCTV operation. We only view images where an incident has occurred on our premises. Any targeted monitoring of staff will take place within the context of our disciplinary procedures;

- **Your Microsoft 365 account** –your mailbox and files may be accessed during and after your employment for the following purposes:

    - personal data breaches or cyber security breaches
    - prevention/detection of crime
    - for the establishment, exercise or defence of legal claims
    - business continuity and operational requirements (if you are on long term sick leave, or you have left the Council) you will be made aware of our purpose in accessing your account unless that notification would prejudice our purpose

The personal data the Council processes about you, and is detailed in this privacy notice, can and may also be used in accordance with the Council's Disciplinary Policy and Procedure or any other relevant policy or procedure that may be in force from time to time.

- We will use your work email address to send you Information we want you to know either for legal or business reasons, for information or action, or to enable you to do your job and/or plan their work effectively. This may also include information which we consider may be of interest to you, for example, information about what the council or your work colleagues have done or are proposing to do.

- The Councils door entry system is logging your time of entry into the Council offices and the entrance used. This location data is collected through the use of your ID cards. This information is kept for 3 months and then is automatically deleted off of the system.

- Your individual use of ICT equipment (computers, tablets, telephones) may be subject to monitoring. ICT can gain access to your account on request to look at your computer activity, mailbox and telecommunications activity. We may do this for a variety of reasons including, monitoring, and improving service delivery, monitoring employee performance, identifying training requirement monitoring compliance with ICT security and usage policies and investigations in connection with disciplinary processes.

- * CCTV is recorded in reception areas, car parks and access roads to monitor security which also captures images of what time you enter and leave the building.

- * Your image will be required to be taken for the creation of an identification card. This is required for staff to access council buildings and shows you are authorised to do so. It also provides evidence of your authority to act in your job.

- ID cards are printed in house and are not outsourced to any third party. This information is processed for the performance of the employment contract as you are required under the terms and conditions of employment to have and wear an identification card.

- your image may be uploaded to your MS365 account, this is optional and is only uploaded if you chose to do so. This can be changed/removed at any time. Staff images are stored on the system securely for the time you are employed and then are deleted off the system when you are no longer employed by the council.

Your personal information may be processed where it is necessary for the purposes of the legitimate interests pursued by us to keep our business data and your personal data secure and confidential and/or defend our legal rights and in some cases, to comply with our duty of care to protect you from harm but not infringe your reasonable expectation of privacy.

Sources of Information

We may collect personal information about you from a number of sources including:

- directly from you
- from members of the public (e.g., complaints)
- from social media
- from an employment agency
- from your employer if you are a secondee
- your doctor
- from referees, either external or internal
- from the Disclosure Barring Service
- from Occupational Health and other health providers
- from pension administrators and other government departments, for example tax details from HMRC
- from your Trade Union
- from providers of staff benefits
- CCTV images taken using our own CCTV systems

We may collect additional personal information in the course of job-related activities throughout the period of you working for us.

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

Volunteering

There may be occasions where you are able to volunteer and provide support to residents of the Dover district. In order to do this, we may request and process your name, email address, contact information and medical/health data. This information will only be requested when the activity or participation of volunteering work could affect an individual's health. This information will be provided from you directly if you wish to apply to be a volunteer.

Lawful bases - our lawful bases for processing your personal data under UK GDPR Article 6(1):

- (a) Consent
- (b) where it is required to fulfil a contract between you and us, or because you have asked us to take specific steps before entering into a contract
- (c)so we can comply with our legal obligations as your employer
- (d)where it is necessary to protect your vital interests or those of another person
- (e)where it is necessary for the performance of our public task which has a clear basis in law or in the exercise of official authority vested in us as Data Controller
- (f)for the purposes of our legitimate interest

Special category data - some of the information that is collected and shared is classified as special category personal data (information about your race or ethnicity, religious beliefs, sexual orientation and political opinions, trade union membership, information about your health, including any medical condition, health and sickness records.

Our lawful bases for processing your special category data under UK GDPR Article 9(2):

- (a) explicit consent
- (b) so we can comply with our legal obligations as your employer
- (c) where it is necessary to protect your vital interests or those of another person
- (f) where it is necessary for the establishment, exercise or defence of legal claims
- (g) where it is necessary for reasons of substantial public interest. Supplemented by the Data Protection Act 2018 Sch 2 Part 2 Para 6 Statutory etc and Government
- (h) where it is necessary for the purposes of preventive or occupational medicine, for the assessment of your working capacity as an employee.

Reasons for processing your personal data:

- Pre employment checks
- for carrying out our obligations and exercising our rights in employment and the safeguarding of your fundamental rights under the Data Protection Act 2018
- to protect your vital interests or those of another person where you are incapable of giving your consent
- for the purposes of preventative or occupational medicine and assessing your working capacity as an employee
- volunteering work you sign up to during your employment at the Council
- business continuity and operational requirements
- Disciplinary, performance and capability purposes
- for the establishment, exercise or defence of legal claims

In addition, we rely on processing conditions at Schedule 1 part 1 paragraph 1 and Schedule 1, part 1, paragraph 2(2)(a) and (b) of the Data Protection Act 2018 i.e. the processing of special category data for employment purposes, preventative or occupational medicine and the assessment of your working capacity as an employee. We have a Data Protection Policy that sets out how this information will be handled.

Criminal convictions and offences - we may only use information relating to criminal convictions where the law allows us to do so. This will usually be where such processing is necessary to act in accordance with our regulatory and other legal obligations and is in accordance with our Data Protection Policy. Although this will be rare, we may also use information relating to criminal convictions where it is necessary in relation to legal claims or to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.

The **lawful bases** we rely to process this data are:

- for the performance of our public task or in the exercise of official authority. In addition, we rely on the processing condition at Schedule 1, part 2, paragraph 6(2)(a) of the Data Protection Act 2018 i.e. this applies to carrying out Disclosure Barring Service checks
- for the performance of a contract. In addition ,we rely on the processing condition at Schedule 1, part 1, paragraph 1 of the Data Protection Act 2018 i.e. the processing is necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on us or on you

Data sharing – in some circumstances, such as under a court order, we are legally obliged to share information. We may also share information about you with third parties including government agencies and external auditors. For example, we may share information about you with HMRC for the purpose of collecting tax and national insurance contributions and with the Cabinet Office as part of the National Fraud Initiative.

We may rely on a number of **exemptions**, which allow us to share information without needing to comply with all the rights and obligations under the Data Protection Act 2018. Please refer to the Kent & Medway Information Agreement for further details on our sharing arrangements.

Retention period - We keep your personal information for the minimum period necessary. The information outlined in this Privacy Notice will be kept in accordance with the retention period(s) unless exceptional circumstances require longer retention e.g. pending legal action. All information will be held securely and disposed of confidentially.

Your right to object – you have the right to object where we are relying on one of the following lawful bases:

- 'public task' (for the performance of a task carried out in the public interest or for the exercise of official authority vested in us); or
- Legitimate interests

You must give specific reasons why you are objecting to the processing of your data. These reasons should be based upon your particular situation. We can refuse to comply if:

- we can demonstrate compelling legitimate grounds for the processing, which override your interest and other rights; or
- the processing is for the establishment, exercise or defence of legal claims.

Your rights – This Privacy Notice should be read in conjunction with our Corporate Privacy Notice, our HR and Recruitment privacy notice which can be viewed here www.dover.gov.uk/privacy this will provide you with further information on your rights.