Your Data: Employees

How we use your information

Employee Records

The Council records and maintains information on all of our employees. This is necessary for the Council, so we can manage our relationship with you, as your employer.

This includes:

- key contact details for you and any emergency contacts you have given us
- information from your recruitment process
- your contractual terms including any variations or extensions
- training and development you have completed
- performance review and development information
- health and safety related information
- information related to your attendance and leave
- your banking details
- declaration of interests and other necessary declarations in relation to employment

The Council has a range of employee related policies, including Supporting Attendance and Wellbeing, Managing Discipline, Managing Performance, Managing Grievances and Dignity and Respect at Work. There are also Health and Safety policies. If you are managed through, or access, an employee related policy, more information about the process, including what information will be created about you, and how this will be used, managed and stored will be given to you at the start of the process.

Use of Council Equipment & Premises

During the course of your employment, use of Council equipment and premises may result in the collection of other data. This includes:

- Dialled telephone numbers and the date, time and duration of incoming and outgoing calls
- Websites visited, including date, times of visit
- Emails sent and received, including dates, times, subject, recipient and sender
- Details of any media files stored on our network
- Clock in times when using time recording equipment
- System login times
- Door entry system recordings
- CCTV footage

This is conducted in accordance with the Council's ICT Acceptable Use and Protective Monitoring Policies. The primary purpose of this is to ensure the protection of our staff, customers, building and ICT infrastructure, systems, networks and data. Information collected may also be used for other purposes, including investigating and managing conduct and for data matching exercises. This will be done in accordance with the Council's Procedures for CCTV, ICT Account Access, or otherwise as we are allowed or required to by law.

The Council also offers employees the opportunity to use facial or fingerprint recognition to log-in to Council ICT devices, where the device specification can support this. This is entirely optional and

staff will always be able to use a password or pin-code if they prefer not to use facial or fingerprint recognition to access their device.

Council systems and records

The Council has a large number of systems in place for keeping records of the work we do, and keeping appropriate records is an important part of everyone who works here's job. In addition to the requirements of the Public Records (Scotland) Act 2011, the Council is also subject to a wide range of specific statutory requirements which set out the type of records we must keep, how we must manage them, and how long we must keep them for. Where there is no specific statutory requirement in place, appropriate creation and management of records it is still a very important of the Council demonstrating accountability.

Records created and generated by Council business, whether created manually or generated by systems will often include names and other details of Council employees. These broader Council records will be retained in accordance with the Council's Records Retention & Disposal Schedule. The primary purpose of these records is to demonstrate accountability for the conduct of Council business. In certain circumstances, information about staff included within our records and systems may also be used for other purposes, including investigating and managing conduct and performance, and for data matching exercises.

The Council uses a range of third-party providers who provide software and telecommunications systems and solutions to the Council. Where necessary to provide the services we have contracted, these third parties will process employee data on our behalf. The Council remains the Data Controller for this information and has contractual arrangements in place to make sure that it is handled properly.

Strategic planning and service improvement

We use employee information in order to provide management information, and to inform service delivery improvement, workforce planning and similar purposes.

Safeguarding public funds

We are legally obliged to safeguard public funds, so employee information may be checked internally for fraud prevention and verification purposes, and may also be shared with other public bodies for the same purpose.

Occupational Health

Information relating to your occupational health may be collected as part of a risk assessment.

If you have ever had an appointment with Aberdeen City Council's current or previous occupational health provider, you may have an occupational health record. Such records are retained by the current occupational health provider. The contents of your medical records are confidential and are not disclosed to Aberdeen City Council but will inform any occupational health reports issued to Aberdeen City Council by the occupational health provider. If the Council change occupational health

provider, these medical records will transfer directly to the new provider and will not pass to Aberdeen City Council.

Information may also be collected from and about you as part of the Council's Health Surveillance programme, to ensure substances you are exposed to are not damaging your health. Results of this surveillance may be shared with line managers and People & Organisational Development for early identification and corrective action.

In circumstances where you engage with the Council's employee assistance provider as a result of a self-referral, relevant personal information will be shared with the provider to allow the counselling service to be delivered. Any information you share with the employee assistance provider will not be passed to the Council.

Employee Photographic ID Badges

The Council issues all staff with a Council Identification Badge, which includes a photograph of you and, which must be worn at all times whilst you are working. The Council does this as part of our duties under Health & Safety law to safeguard our staff, as well as secure access to our buildings.

The Council publishes ID badges alongside work contact details on our Employee Finder on the Council's internal intranet site. This is to promote efficient and effective working between our staff. The Council does this because we have a legitimate interest in supporting our staff to know who each other are, as an employer who has large number of staff, working across multiple sites.

Attending Council or Committee or authoring Committee reports

Some employees may be required, as part of their duties, to attend or speak at Aberdeen City Council, Committees or Sub-Committees. If these meetings are web-cast then images of the meeting will be published on the Council's website.

If you are the author of a committee report or named as the contact point in that report, your name, service and work telephone number will be published on the committee report on the Council website.

Acting as an Agent for the Council

Some employees may, as part of their duties, act as an agent on the Council's behalf.

If you act as an agent in this way then your name, service and job title may be disclosed in accordance with the requirements of the process. Where the law requires that a public register is maintained your name, work email address and work telephone number may also be disclosed.

Freedom of Information Requests

The Council is subject to freedom of information ("FOI") legislation. Often, we receive requests which seek disclosure of information about members of staff. Such requests are assessed carefully, and we will only release staff information in response to FOI requests if doing so is compatible with our obligations under data protection law.

As a general rule, we will not release names or information which could identify employees unless they are a Chief Officer. We will never voluntarily release non-work-related information about any

member of staff such as home address, nor will we voluntarily release information where this relates to the member of staff being a service user rather than in their capacity as an employee. We will seek the views of current members of staff as to any such release.

Employee Benefits

Aberdeen City Council offers a benefit scheme for employees, run by a third party. You can choose to have an account and to take up benefits using the scheme. If you choose to open an account to access employee benefits, we will verify certain personal details with the benefits scheme provider, in order to confirm your eligibility for the scheme. We may confirm further information to third parties to determine your eligibility for products or services. The Council will access anonymous information from third parties about the uptake of various benefits as part of our ongoing evaluation of the benefits provided.

Sharing with HMRC, Regulators and Enforcement Bodies

We are legally obliged to share certain data with other public bodies such as HMRC; we will also generally comply with requests for specific information from other regulatory and law enforcement bodies.

Sharing with the relevant Pension Fund

Where an employee is a member of one of the Council's pension schemes, we need to share information to ensure appropriate contributions and benefit calculations can be made.

Sharing of Payroll Deductions

In certain circumstances relevant personal data may be shared with third parties in respect of processing payroll deduction made in respect of such items as salary sacrifice contributions, charitable giving arrangements, payments made to satisfy court orders, AVC scheme contributions, trade union subscriptions or credit union contributions.

Sharing with Professional Regulators

Depending upon the nature of your role, relevant information may be shared with appropriate professional regulatory bodies such at the Scottish Social Services Council (SSSC) or General Teaching Council for Scotland (GTCS).

Sharing with Qualifications Authorities

Where workplace assessment for a qualification is undertaken, personal data may be shared with the appropriate qualifications authority, such as the Scottish Qualifications Authority and City and Guilds, for the processing of results and issuing of qualifications.

Sharing with the Health & Safety Executive

Personal information gathered in relation to incidents or near misses at work, claims for recompense for Display Screen Equipment, risk assessments and personal evacuation plans may be required to be shared with the HSE.

Sharing with the Council's Insurers

Your personal details may be shared with the Council's insurance provider for the purposes of insurance policies held by the Council in respect of Employer's Liability Insurance, Indemnification of employees and other insurance purposes as necessary.

Sharing with The National Fraud Initiative in Scotland

The Council is obliged to participate in the National Fraud Initiative in Scotland and in terms of this passes information on staff, primarily payroll data, to Audit Scotland for data matching to detect fraud or possible fraud. Details of this exercise can be found on Audit Scotland's website at http://www.audit-scotland.gov.uk/our-work/national-fraud-initiative.

Sharing with the Court

If at any time during or subsequent to your employment you exercise your rights to enter into a dispute via the courts system, including employment tribunal, we may be required to share information in relation to your employment relationship with the courts or legal representatives as required.

Sharing with External Workplace Accreditation Bodies

If workplace assessment is required to obtain external accreditation, for example Investors in People, limited personal data may be shared with the accrediting body for the purpose of selecting employees for evidence gathering interviews.

How long we will keep your information for

Most of the information within each employee's file is kept for the current year plus six more years, from the date you leave Aberdeen City Council.

If during your employment with the Council you work or have worked with children or vulnerable adults, then most of information within your employee file will be kept for the current year, plus twenty-five years more years from the date you leave the Council.

We keep some information about our employees for shorter or longer periods of time. For example, we keep basic details about each of our employees for a longer time, so we can evidence employment and for pension and health surveillance purposes.

The Council's Retention & Disposal Schedule sets out the retention periods for any information about you which won't be destroyed at the same time as your employee file.

Your rights

Aberdeen City Council is the Data Controller for this information. You've got legal rights about the way the Council handles and uses your data, which include the right to ask for a copy of it, and to ask us to stop doing something with your data. Please contact the Council's Data Protection Officer by email on DataProtectionOfficer@aberdeencity.gov.uk or in writing at: Data Protection Officer, Marischal College, Aberdeen, AB10 1AB. See more information about all of the rights you have. You

also have the right to make a complaint to the Information Commissioner's Office. They are the body responsible for making sure organisations like the Council handle your data lawfully.

Please note if your complaint is not about data protection but instead is about an employment matter, then this should be raised initially with your line manager and if necessary through the Council's grievance procedure.

Our legal bases

Whenever the Council processes personal data we need to make sure we have a basis for doing so in data protection law. We understand our basis in data protection law to be Article 6(1)(b) of the General Data Protection Regulation (GDPR) because processing your personal information is necessary for us manage our relationship with you, as your employer. As outlined above, there are also times where we are required by law to process your information, in these cases, our legal basis is Article 6(1)(c), and times where we are processing your information based on 6(1)(f) our legitimate interest. In cases where employees make an active choice to use fingerprint or facial recognition to access their Council ICT devices, our legal basis is Article 9(2)(a). Employees can change their mind about using facial or fingerprint recognition to access their device at any time.

As part of this relationship, the Council is also likely to process special categories of personal data. The Council understands our legal basis for doing so as Article 9(2)(b) of the GDPR as processing is necessary for carrying out our obligations in the field of employment.