East Ayrshire Council
Comhairle Siorrachd Àir an Ear

Data Protection Policy – Our handling of personal information

Who are we?

East Ayrshire Council is a Scottish local authority constituted under the Local Government etc. (Scotland) Act 1994. Our main offices are at Council Offices, London Road, Kilmarnock, KA3 7BU.

Why do we have a data protection policy?

We want users of our services to feel confident about the privacy and security of their personal information. We are aware that the proper handling of this information is vital.

We will take all reasonable steps to ensure that we comply with the requirements of the data protection law, particularly in relation to the use of your personal information by us that is compliant with data protection laws and/or the prevention of any unauthorised access to your personal information.

How Our Data Protection Policy applies

What is "personal information"?

When we talk about "personal information", we are referring to "personal data" which is any information that identifies someone as a living, private individual or could do so if combined with any other information.

What information do we hold about people?

In order to provide services, we have and use a large amount of personal data about people. This information could be about current, past and prospective employees, suppliers, clients and service users/customers.

We may hold information such as someone's name, address and date of birth, but we could have sensitive information such as information about his/her health, racial or ethnic origin, or any criminal offences that he/she may have committed. The type of information that we have will depend upon the reason why we need the information i.e. to provide a service to someone.

Further information regarding our responsibilities with regards to sensitive data is contained at Annex A.

How do we get personal information?

In most cases, the information that we have will come from the person concerned, for instance when applying for a service from us. However, the information could come

from the person's legal representative, partner, relatives and other agencies such as the police, other Councils, the NHS or the HMRC. We will ensure that the individual concerned will be aware that we have received and are using their personal information unless there is a good reason not to do so set down in data protection laws.

Why do we need someone's information?

We will only use personal information where we need to do so in connection with the provision of services or other Council business for instance where necessary to do so in connection with

- a statutory function or;
- where we are under an obligation to use the personal information in terms of law or;
- where we need to do so in order to perform a contract between you and the Council or
- where we need to do so to protect someone's vital interests or;
- if someone else has a legitimate interest in relation to obtaining the personal information. However, we will only do this where we are satisfied that your own rights and freedoms do not take precedence over the interests of the other person/organisation.

There may be cases where what we are offering are additional services intended to make a process easier for people but is not necessary for our functions, we will ask you for your consent to use your information in this way. In those cases, you will be entitled to withdraw your consent at any time.

Who could we give your personal information to?

From time to time, we will share someone's personal information with other bodies. There may be times when we will share someone's information without consent, for example, with the police, the NHS or other agencies. We will only share your personal information in compliance with data protection laws.

How do we handle someone's personal information?

When we refer to "using" personal information this has the same meaning as "processing" in terms of data protection laws. This is where we collect, record, organise, structure, store, adapt or alter, retrieve, consult, use, disclose, disseminate or otherwise make available, restrict, erase or destroy any of your personal information.

Before we start to use your personal information that you have provided to us, generally, we will let you know that we are doing so and provide other information to you that will make things clear to you. If we receive your personal information from someone else, generally, we will let you know that we have received your information and what we are doing with it. Thereafter we will let you know of any new uses of your personal information as soon as we can.

We will not inform you about the uses of your personal information and other relevant information if there is a good reason not to do, set down in data protection laws, such as when it could result in harm to someone else.

How long will we keep your information?

We are aware that we must not keep personal information longer than is necessary for our purposes. Sometimes, law sets down these time limits. In that case, we must comply with those specified time limits.

However, in most cases this relates to where we have a business need to keep the personal information although it may be that we are not actively using the information. This usually depends upon whether anyone has continuing interest (such as auditors) in the information or whether we have to maintain a record as to why we processed the information in the first place. These time limits are set down in statute. This could be, for instance,

- at least 6 months in relation to people who have applied for and have been unsuccessful in relation to a post within the Council (being the maximum period for them to complain to the Employment Tribunal) or;
- a period of at least 5 years from when the potential cause of any dispute arose, where someone retains the power to potentially raise proceedings against the Council for payment of money,
- if any action is raised against the Council, the personal information will be kept until the conclusion of that action even if the normal period for holding the information has expired or;
- there may be times when we wish to archive personal information because it is in the public interest to do so. However, we would put appropriate safeguards in place to protect your rights and freedoms.

We maintain Retention Schedules that set out the periods of time that we apply to keeping particular information. If you wish to get more information about the specific time limit for particular information, you can

- ask to see the relevant retention schedule or
- exercise your right to be told about our use of your personal information (the right of access – see later).

What are your rights in relation to our use of your personal information?

In terms of data protection laws, you may have some or all of these following rights. The rights in italics only apply in certain circumstances or are restricted and so may not be fully available to you.

You have the right to ask us to:

- confirm that we are using personal information about you, detail what that information is, to whom we have disclosed your information and a copy of the information that we have about you (The right of access)
- correct any incorrect or misleading personal information that we have about you (The right to rectification)

- *stop using any or all of your personal information (The right to object)*
- *to delete to destroy your personal information (The right to erasure including the right to be forgotten) and*
- *stop using your personal information until we can look into correcting your personal information or our justification for using your personal information or to stop us deleting your personal data where you need it in connection with any legal claims (the right of restriction) and*
- *pass your personal information to someone else (the right to data portability (this only applies where we are using your information in relation to a contract or with your consent).*

When exercising any of the rights, you should try to be as specific as possible about the personal information concerned.

Further guidance about how to exercise these rights can be obtained from our Data Protection Officer:

- By phone on 01563 57 6094
- By email using information.governance@east-ayrshire.gov.uk

Our Governance arrangements

Our data protection commitment

We know that if we do not comply with data protection laws, including protecting the information, we will lose the trust and confidence of the public and our partners.

Data protection laws set down rules that we must follow when collecting and using personal information. These rules are called the data protection principles.

To comply with these principles, we must take steps to ensure that all personal information is:

- lawfully, fairly and transparently;
- held and used for specified purposes;
- adequate, relevant and limited to what is necessary for our purposes
- accurate and up to date;
- not kept any longer than necessary; and
- kept secure.

.

Who is responsible for data protection?

The Council as a whole, has a responsibility for compliance with data protection laws. However, it places specific responsibilities on:

- the Chief Executive and Executive Directors, who will implement and enforce this policy across the Council and ensure that employees receive the appropriate training;
- the Data Protection Officer will provide appropriate training to elected members on data protection laws in relation to their roles;

- our Corporate Information Governance Group who will provide guidance and advice on operational matters such as ensuring security of personal information, such as how we store information, who should have access to information and how we transfer information to other bodies or agencies;
- line managers, who will make sure that employees are aware of and comply with their responsibilities and;
- Individual employees, who are to comply with their data protection responsibilities.

Who is our Data Protection Officer and what are their responsibilities?

We have a Data Protection Officer (DPO) to:

- help and advise us on meeting our data protection obligations
- check our compliance with data protection laws and our policies, including carrying out audits and ensuring that we provided training to our employees in accordance with the law and this policy
- provide advice to us to help us carry out any assessments that we may make in connection with data protection compliance.

If you have any concerns or enquiries about the way that we use your personal information or wish to exercise any of your rights (see later) you can contact the DPO direct. The DPO's details are as follows:

The Data Protection Officer
Governance Services
Council Headquarters
London Road
Kilmarnock
KA3 7BU

By email to: information.governance@east-ayrshire.gov.uk

By phone on: 01563 57 6094

How do we ensure that what we are compliant with data protection laws?

In relation to the holding and use of personal information, we are aware that our responsibilities apply all of the time that we hold and use the personal information. We appreciate that we must ensure that we treat all personal information correctly.

We will keep in mind that your rights and freedoms go further than respect for your privacy. The appropriateness of all decisions or actions taken by us will be dependent upon the reliability (adequacy, accuracy, and relevancy) and accessibility of your personal information.

Before we start to use your personal information for

- a new purpose or
- make changes to the existing way that we already handle information or

- change the means that we use to process personal information

involving a high risk to your rights and freedoms as an individual, we will carry out a privacy impact assessment (where necessary) at the earliest possible stage in the planning process.

When carrying out these assessments or dealing with any data protection matters, we will ensure that we involve the DPO, fully, at the earliest opportunity.

We will ensure that any contractors, who are providing services on our behalf, treat personal information in the same way that we do.

How do people find out about changes to our data protection policy?

We may change our data protection policy from time to time. We will publish any new or amended policy on our website.

More Information

You can get details of our notification to the Information Commissioner and information on data protection laws published by the Information Commissioner at www.ico.gov.uk.

Annex A

East Ayrshire Council – policy statement and additional safeguards on processing special category data and personal data relating to criminal convictions and offences

Introduction

With effect from 25 May 2018, data protection law requires controllers who process special category (i.e. sensitive) personal data, (or personal data relating to criminal convictions and offences) under various parts of the Data Protection Act 2018 to have an "appropriate policy document" in place setting out a number of additional safeguards for this data.

More specifically, the law states that:

"The controller has an appropriate policy document in place in relation to the processing of personal data… if the controller has produced a document which -

> (a) explains the controller's procedures for securing compliance with the principles in Article 5 of the GDPR (principles relating to processing of personal data) in connection with the processing of personal data in reliance on the condition in question, and
>
> (b) explains the controller's policies as regards the retention and erasure of personal data processed in reliance on the condition, giving an indication of how long such personal data is likely to be retained."

This document is the policy adopted by East Ayrshire Council in relation to this processing.

Policy Statement

1: Lawfulness, fairness and transparency:

All data flows into and out of the Council are being assessed to determine the legal basis under which that data is processed and the results of the assessment are being documented in an Information asset Register. We are satisfied that we will have a legal basis for holding the personal data we hold, and that we will also have a valid legal basis for disclosing this personal data to third parties where this happens. Privacy notices have been drafted to comply with GDPR requirements (and to reflect the legal basis of processing). Please see the Council website for further details.

2: Purpose limitation:

The purposes for which data are collected are clearly set out in the relevant privacy statements. A limited set of data is required for research and archiving purposes; the Council has put in place appropriate safeguards for these activities as required by Article 89 of the GDPR.

3: Data minimisation:

In assessing the data flows, the Council is also taking the opportunity to assess the need for each of the data fields in question and will cease to capture unnecessary data.

4: Accuracy:

The Council checks data for accuracy and, where any inaccuracies are discovered, these are promptly corrected and any third party recipients of the inaccurate data notified of the correction.

5: Storage limitation:

The Council only keep personal information for the minimum period amount of time necessary. Sometimes this time period is set out in the law, but in most cases it is based on business need. We maintain a records retention and disposal schedule which sets out how long we hold different types of information for. You can view this on our website at www.east-ayrshire.gov.uk

Ongoing management of the Council's records and information is subject to the provisions of our Records Management Plan, which was developed in terms of the Public Records (Scotland) Act 2011 and approved by the Keeper of the Records of Scotland. The Records Management Plan sets out, in much greater detail, the provisions under which the Council complies with its obligations under public records legislation, data protection and information security and is complementary to this policy statement.

6: Integrity and confidentiality:

The Council has an Information Security Policy which sets out roles and responsibilities within the organisation in relation to information security. All staff are required to take information security training and this is refreshed bi-annually. Our ICT systems have appropriate protective measures in place incorporating defence in depth and the systems are subject to external assessment and validation. We have policies and procedures in place to reduce the information security risks arising from use of hard copy documentation.