Agenda Item

Report

Report to:	**Executive Committee**
Date of Meeting:	**1 May 2019**
Report by:	**Executive Director (Finance and Corporate Resources)**

Subject:	**Data Protection Policy** **Charges for Access to Information**

1. Purpose of Report

1.1. The purpose of the report is to:-

- request approval for a revised Data Protection Policy to replace the existing Privacy Policy
- request approval for changes to the Council's Charging Policy in respect of requests for information made under data protection legislation

2. Recommendations

2.1. The Committee is asked to approve the following recommendations:-

(1) that the revised Data Protection Policy attached at Appendix 1 be approved as a replacement for the existing Privacy Policy; and

(2) that the proposed changes to the Council's Charging Policy, outlined at section 4 of the report, in respect of requests for information under data protection legislation be agreed.

3. Background

3.1. At its meeting on 2 February 2011, the Corporate Resources Committee introduced a fee for the processing of subject access requests under the then Data Protection Act 1998.

3.2. On 8 February 2012, the Executive Committee agreed the adoption of a Privacy Policy as part of its overall information governance strategy. This policy set out the Council's approach to achieve compliance with the Data Protection Act 1998 and its governance arrangements for data protection matters.

3.3. On 25 May 2018, the General Data Protection Regulation (as supplemented by the Data Protection Act 2018) (the GDPR) came into force and now sets out the rules for the general use of personal information by the Council. The GDPR, however, does not apply to the circumstances set out in paragraph 3.4.

3.4. On the same day, Part 3 of the Data Protection Act 2018 (the DPA) came into force. This legislation applies, to situations where the Council, is acting as a law enforcement authority and where it is processing personal data for a law enforcement purpose.

3.5. The Council has had to revise a considerable amount of existing documentation and to devise new forms, guidance and processes to take to take account of the new legislation. This Policy is the last major step in this programme of work.

4. Charging for requests for information

4.1. In 2011, the Council set the charge for subject access requests at the maximum figure of £10 permitted under the 1998 Act.

4.2. In terms of the GDPR, an individual is still entitled to make a request for any personal information held by the Council. The period for compliance with these requests has reduced from 40 calendar days to 1 month (which is being taken as referring to 30 calendar days).

4.3. The GDPR states that such requests must be free of charge, except in the circumstances set out in 4.4 of this Report. Accordingly, the Council is no longer allowed to charge the £10 fee for subject access requests and the Charging Policy must reflect that.

4.4. Limited circumstances remain in which the Council may levy a fee under the GDPR. This ability is restricted to requests that are manifestly unfounded or excessive, particularly because of their repetitive character. The fee may take account of the administrative costs incurred to provide the information. Alternatively the Council may refuse to provide the information. The ability to charge a fee may be subject to limits made by the UK Government under section 12 of the Data Protection Act 2018 (which has repealed the previous 1998 Act in full). There are no such limits in force as yet.

4.5. The DPA 2018 contains similar provisions regarding charges in respect of requests for information made under it.

4.6. In terms of the existing Charging Policy, the decision to charge/waive fees is delegated to the Executive Director (Finance and Corporate Resources) and those authorised by him. Given the legislative changes, it is suggested that:-

(a) the fee of £10 for subject access requests be removed and that
(b) the discretion to levy a fee or to refuse a request meeting the criteria outlined in 4.4 above under the GDPR/DPA be delegated to each Executive Director, in respect of requests received by their Resource. The level of fee will be subject to any Regulations regarding limits etc. made by the UK Government.

5. Data Protection Policy

5.1. The Data Protection Act 2018 (the DPA) has introduced additional safeguards to protect the rights and freedoms of data subjects in respect of information caught by the special category personal data definition, which were not contained within the previous legislation. These safeguards apply to the processing of special category data under the GDPR as well as the DPA. Special category personal data is that relating to race, politics, religion, union membership, health or sexual orientation.

5.2. In order to meet one of these safeguards, the Council must have an “appropriate policy document” in place. Paragraph 39 of Part 4 of Schedule 1 to the DPA (GDPR) and section 42 of the DPA (law enforcement) sets down the required contents of this policy. The Council’s existing Privacy Policy approved in 2012, with some amendments will meet the required content. Consequently, the Privacy Policy has been revised and updated to include any additional required content and the draft Policy is attached to this report for consideration by the Executive Committee.

5.3. In order to make it more readily accessible for members of the public who may wish to obtain a copy of the policy, it has been renamed as the “South Lanarkshire Council Data Protection Policy”.

6. Employee Implications

6.1. None.

7. Financial Implications

7.1. A small amount of income, circa £600 per annum, was generated by former arrangements and this will no longer be received.

8. Other Implications

8.1. There are no implications in terms of risk or sustainability.

9. Equality Impact Assessment and Consultation Arrangements

9.1 The draft Data Protection Policy has been approved by the Council’s Information Governance Board on 14 May 2018.

9.2 In accordance with the requirements of the GDPR, the Council’s Data Protection Officer has been consulted and has assessed the draft Policy as compliant with the GDPR.

Paul Manning
Executive Director (Finance and Corporate Resources)

9 April 2019

Link(s) to Council Values/Ambitions/Objectives

- Accountable, effective, efficient and transparent

Previous References

- Corporate Resources Committee, 2 February 2011
- Executive Committee, 8 February 2012

List of Background Papers

- None

Contact for Further Information

If you would like to inspect the background papers or want further information, please contact:-

Bill Dunn, Information Compliance Manager
Ext: 4564 (Tel: 01698 454564)
E-mail: bill.dunn@southlanarkshire.gov.uk

APPENDIX 1

Data Protection Policy – Our handling of personal information

Who are we?

We are South Lanarkshire Council, a Scottish local authority constituted under the Local Government etc. (Scotland) Act 1994. Our main offices are at Council Offices, Almada Street, Hamilton, ML3 0AA.

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 that the use of your personal information by us is compliant with data protection laws and that any unauthorised access to your personal information is prevented.

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.

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 made 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 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 which are intended to make a process easier for people but are 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, what we are doing with it and the other information within 1 month of receiving your information. After then, 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 set down in data protection laws such as when providing information 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, the law sets down 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 we may not be actively using the information. This usually depends upon whether anyone has continuing interest in (such as auditors) or rights to take action of any sort against us in relation to the purpose the information is being used for. These time limits are set down in statute. This could be, for instance,

- at least 6 months for people who have applied for a job with the Council and have been unsuccessful (the maximum period for them to complain to the Employment Tribunal) or
- a period of at least 5 years from the date when a 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 period of 5 years has passed 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 keep 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 may be 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, provide detail about that information, confirm to whom we have disclosed your information and obtain 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)
- delete or 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.

We have guidance about how to exercise these rights. You can get a copy of it

- By mail or email to our Data Protection Officer, whose contact details are given later
- By phone on 0303 123 1015
- By email using dp@southlanarkshire.gov.uk

Alternatively, you can get guidance (and apply to exercise the rights) on the Data Protection page of our website.

Our Governance arrangements

Our data protection promise

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 and for what?

We, the Council, as a whole, have a responsibility for compliance with data protection laws. Specific responsibilities have been passed to:

- the Chief Executive and Executive Directors, who will implement and enforce this policy across each Resource and ensure that employees receive the appropriate training
- the Executive Director (Finance and Corporate Resources) who will provide appropriate training to elected members on data protection laws in relation to their roles
- our Information Governance Board who will provide guidance and advice on operational matters such as ensuring security of personal information, how to store information, who should have access to information and how to 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 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 have assigned responsibilities and 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.

We will give the DPO independence to carry out these tasks and ensure that the DPO is able to carry out these tasks freely and impartially.

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

The Data Protection Officer,
Administration and Legal Services
Finance and Corporate Resources
Floor 11
Council Offices
Almada Street,
Hamilton
ML3 0AA

By email to: dp@southlanarkshire.gov.uk

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

We are aware that our responsibilities apply all of the time that we hold and use your personal information. We appreciate that we must have checks in place to make sure 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.

Further, we will carry out regular reviews of the ways that we collect and use personal information to make sure that we are still complying with data protection laws. We will do this by carrying out an assessment at regular periods determined by the sensitivity of the personal information involved.

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 any 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.