eastsussex.gov.uk

East Sussex County Council

Data Protection - Guidance for Employees

June 2019
V.8

Document Owner/Contact	ESCC IG Lead
Date last reviewed	June 2019
Next Review Due	March 2020
Version	V.8.0
Target Audience	ESCC Staff, members and other agencies handling ESCC information
Security Classification	Official - Disclosable

Version history

no	Issue date	Summary of Changes
1	Nov 2004	updated contact details
2	May 2007	updates Liaison Officers; corrected links to online documents
3	April 2008	Revised and expanded guidance, update to Liaison Officers; format revised to meet new publishing standards (incl removal of direct links to intranet)
4	March 2014	Updates to job titles and contacts
5	March 2014	Update to Section 29(3) procedure. Update regarding information sharing protocol in cases of child abuse
6	Aug 2017	Update to job titles and contacts
7	Feb 2018	Update to take account of new data protection legislation and expand applicability to all those handling personal data on behalf of the Council
8	June 2019	Update to job titles, contacts and removal of Notification section

1. Introduction

Data Protection legislation places obligations on all those who process personal data. Legislation includes the following terms:

- *processing* includes collecting, using, storing, disclosing and disposing of information
- *personal data* (or information) means any information relating to an individual ('data subject) who can be identified directly or indirectly by an identifier such as name, ID number, location data (e.g. address), online identifier (e.g. IP address) or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual.
- *special category data* - sensitive personal data (which requires extra protection) including any information that may identify an individual's:
    - racial or ethnic origin,
    - political opinions,
    - religious or philosophical beliefs,
    - trade union membership,
    - health,
    - sex life/orientation
    - genetic/biometric identifier
    - criminal convictions

2. Purpose

The purpose of this document is to outline the responsibility of every individual involved in processing personal data on behalf of ESCC, in line with data protection legislation and to provide basic information about disclosures.

If you are in any doubt about how the legislation affects you, seek advice from your Information Governance Officer – details at section 13.

3. Scope

Data Protection legislation defines the following roles:-

Data Controller – the person or organisation that determines the purposes and means of the processing of personal data i.e. decides how and why data is used. This will often be the County Council

Data Processors – the person or organisation that processes data on behalf of the controller

Data Subjects – the individuals whose information is collected and processed (for example clients, members of the public, members of staff)

Data Recipients – any person or organisation to whom data is disclosed.

4. Policy statement:

All personal information must be collected, processed, maintained and disclosed in accordance with the following principles – personal data shall be:

- processed lawfully, fairly and in a transparent manner
- collected and used for specified, explicit and legitimate purposes and not further processed in an incompatible way ('*purpose limitation*')
- adequate, relevant and limited to what is necessary for the purpose for processing ('*data minimisation*')
- accurate and where required, rectified without delay ('*accuracy*')
- not be kept in an identifiable form for longer than necessary ('*storage limitation*') i.e. in line with ESCC retention schedules
- information must be appropriately secured/protected against unauthorised or unlawful processing, accidental loss, destruction or damage using appropriate technical or organisational measures ('*integrity and confidentiality*'). This includes:
  - *using appropriate means of transmitting data*
  - *secure storage / disposal of personal information*
  - *where processing is sub-contracted or outsourced (e.g. payroll, disposal of confidential waste paper) there must be suitable Data Protection clauses in the contract*

  See the Council's Information Security Policy suite for more information on securing personal data.

Personal information must also:

- be processed in accordance with the rights of data subjects e.g. right of access, right of erasure, rectification, restriction, portability and the right to object to certain processing (see section 7.)
- not be transferred to countries outside the European Economic Area without adequate protection

All staff and Members may have access to personal information and must all ensure that it is processed in accordance with the requirements of data protection legislation.

5. Data Protection By Design

Whenever you are introducing a new policy, procedure, system or database that will involve personal data you must complete a Data Protection Impact Assessment.

A Data Protection Impact Assessment (DPIA) is a tool that you can use to identify and reduce the privacy risks in your service area. A DPIA can reduce the risks of harm to individuals through the misuse of their personal information. It can also help you to design more efficient and effective processes for handling personal data.

A DPIA can also be used as a tool for evaluating risk levels on existing processes, procedures and systems.

6. Data Subject Rights

Any person wishing to exercise their rights under data protection legislation must do so by completing a form which can be accessed on the council's website or by emailing or writing to the Council - details of which can also be found on the ESCC Website.

Individuals' requests must be processed within 1 month of receipt of the request unless the request is complex* (or if multiple requests are received from the same data subject) - in this case a 3 month deadline for addressing the request will apply. For complex requests likely to take over 1 month, the data subject must be notified of this within the initial 1 month period.

*Responding to "Complex" Requests

There may be instances when a request for information is more complex, e.g.:

- it involves retrieval and appraisal of information from multiple sources
- it involves the retrieval of large volumes of information for one data subject which are difficult to separate from information relating to other data subjects
- it is one in a series of requests from the same individual
- it involves the release of third party data for which consent has been refused or cannot be obtained

In these cases your Information Governance Officer will be able to advise on the approach to take and whether or not the extra time can be allowed to complete the request.

Right of Access

The Council has a long-standing policy of access to information, especially in relation to access to case records.

Under data protection legislation every individual has the right of access to information relating to them. This right is called Subject Access. Any person wishing to make a Subject Access request must do so by completing a form as above. You must not disclose personal information verbally on request.

In some circumstances the individual or their representative may make an appointment to view their record with a member of staff who can then discuss or explain any issues or concerns. This is the preferred course of action where staff within ASC or CSD feel that it will assist the data subject come to terms with sensitive and difficult personal information. Whether or not to accept the offer of this service is a personal choice for the applicant.

If an individual has nominated another person (e.g. a solicitor) to make a request on their behalf, they must also provide written consent. Parents may make requests on behalf of their children. But if the child is 13 years or older, the child must also provide written consent for the parent to make the application on their behalf.

Where an adult lacks mental capacity, a nominated person may make an application on their behalf. In these circumstances, the person making the application must have proof of a valid Lasting Power of Attorney or an Enduring Power of Attorney or proof of Court-appointed Deputyship.

No information relating to any other person (other than the individual requesting the information) will be disclosed as part of a subject access disclosure.

Any information that may prejudice the prevention and detection of crime may be exempted from disclosure. There are also a number of other less often used exemptions available. Staff with any concerns about the release of personal data, even to the data subject themselves, must contact their Information Governance Officer, who will be able to offer advice.

Right of erasure

Data subjects also have the right to request that the data we hold about them is deleted - this right allows individuals to request that their personal data is deleted where there is no justification for its continued use. This right only applies when:

1. The data is no longer necessary for the reason(s) for which it was originally collected
2. The data subject provided consent for the Council to process their data but have subsequently withdrawn this consent
3. That data subject has objected to the Council processing their data and we have no overriding grounds for continuing to process it
4. The data was processed in breach of the GDPR i.e. it was unlawfully processed
5. There is a legal requirement to erase the data
6. The data was collected with parental consent when the data subject was a child and they no longer wish for their data to be held

There are some circumstances where the Council doesn't have to comply with a request for erasure:

1. When the Council has a legal obligation or it is part of our official authority to process the data
2. For public health reasons
3. For certain archiving activities
4. When we need the data in connection with a legal claim

For support in deciding whether the right to erasure should be applied, contact your Information Governance Officer.

Right to rectification

If data subjects believe that any of the personal data we hold about them is inaccurate or incomplete they are entitled to ask for it to be rectified. If an individual believes certain data to be incomplete we must look at this in the context of why we are processing the information and take necessary steps to supplement the information we hold in order to make it complete.

Right to restriction

In certain circumstances data subjects have a right to request that we temporarily restrict processing and access to their data. This will apply:

1. Whilst establishing accuracy of data, if a data subject has contested this
2. Whilst we follow up any objection raised by a data subject to the Council processing their data.
3. When data has been processed unlawfully but the data subject does not want us to erase it and have asked, instead, for us to restrict processing of the data.
4. When we no longer need the data but the data subject has advised us that they need it in connection with a legal claim.

The right to restrict data doesn't apply if:

1. The processing is necessary for the Council in connection with a legal claim
2. It is necessary for the protection of another person
3. There are substantial public interest reasons for continuing to process the data

For support in deciding whether the right to restriction should be applied, contact your Information Governance Officer.

Right to portability

Data subjects have a right to request that their data be transferred electronically to another organisation. Contact IT&D and/or your Information Governance Officer for further advice on how such requests might be fulfilled.

The right to portability only applies when:

1. The data subject themselves supplied the information and provided consent for the processing; or
2. The data is being processed as part of a contract to which the data subject is party; and
3. The data is held electronically (not in paper files)

Right to object

Data subjects have the right to object to their information being processed in the following circumstances:

- If the legal justification we have outlined is that processing is necessary either to a) perform a task carried out in the public interest or b) as part of the organisations

official authority or legitimate interest and the data subject feels this is not applicable.

- In the case that we retain information in defence or potential defence of a legal claim but the data subject believes there are insufficient grounds to do so.

Data subjects also have a right to object to their data being used for direct marketing purposes at any time and we must cease processing for this purpose. Examples of direct marketing conducted by the Council might include distribution of leaflets, providing information on services that might be relevant to the data subject.

Where the Council uses IT systems to make automatic decisions based on personal data e.g. calculate eligibility to receive a service, unless an exemption applies^ data subjects have a right to object and:

- request human intervention in the decision making
- be able to express their point of view
- obtain an explanation of how a decision has been reached
- challenge the decision

^Data Subjects do not have a right to object to 'automated decision making' if:

- it is necessary to fulfil a contract in which they are party
- automated processing is authorised by law
- we have explicit consent

Where we are using data for research purposes individuals have the right to object unless the research is being undertaken in the wider public interest which outweighs a data subjects right to privacy.

7. Third party requests for disclosure

Where you receive a request for personal information from an outside organisation or individual, you must be satisfied that the information requested falls within one of the restrictions applicable under data protection legislation, that allow sharing of personal data in certain exceptional circumstances.

On most occasions, such requests will be for disclosure of information that is considered necessary for the purposes of:

- Prevention, investigation, detection or prosecution of criminal offences including threats to public security
- National security
- Monetary, budgetary and taxation matters (e.g. assessing or collecting taxes), public health and social security

On some occasions individuals or organisations may request personal data for the purpose of:

- Protection of judicial independence and judicial proceedings
- Prevention, investigation, detection or prosecution of breaches of ethics
- Protection of the data subject or the right and freedoms of others
- Enforcement of civil law claims

Those disclosing information must be satisfied that the disclosure is necessary, and that if we did not disclose the information the non-disclosure would be likely to prejudice the above aims. Requests should always be made in writing, and the person requesting disclosure should provide the information listed below:

- name and contact details of person or organisation making the request,
- date of request,
- details of the person to whom the disclosure relates, and
- the reason the information is required.

Such requests are likely to be made where the other authority does not have specific powers to obtain the information, for example

- other local authorities and / or Dept. for Work & Pensions investigating benefit fraud
- police forces making enquiries about serious crime incidents or missing persons. *Note that any requests made by police officers must be made in writing and authorised by an officer of at least the rank of Inspector or an equivalent police staff of SPA grade 11 or above.*

All such requests should be passed to the Customer Services Team (via the Customer Services System) for processing. However, if for any reason this does not happen, staff must record any steps taken to verify the identity of the requester, and make a record of the information disclosed. Staff must ensure a copy of the above is passed to their Information Governance Officer, who should in turn pass it to the Customer Services Team to enable them to maintain the central record,

The Customer Services Team process and record all such requests. This is to ensure compliance with Data Protection legislation and also to ensure an accurate record is maintained. This will protect staff and officers from accusations of unlawful disclosure and also enable the Council and, potentially, the Information Commissioner to assess any disclosure decision.

Staff should be aware that there is a current Information Sharing Protocol between ESCC, WSCC, Brighton & Hove, Sussex Police and the Crown Prosecution Service in relation to the sharing of information in the investigation and prosecution of child abuse cases in Sussex. Where staff are asked for information in such cases by any of the above organisations it will usually be possible to pass information with the minimum of delay and without the involvement of Information Governance Officers. However, staff must still be satisfied of the identity of the requester and organisation and the validity of the request. Staff must also make a retrievable record of the disclosure process for the same reasons as outlined above.

If in doubt about any requests for information, please contact your Information Governance Officer or the Data protection Officer

8. Information sharing protocols and service level agreements

Information must only be disclosed under information-sharing protocols and service level agreements where the person processing such a request can be confident that the disclosure in question can be supported by a specific statutory basis (or exemption). It is every staff member's responsibility to ensure they are confident of the lawfulness of any disclosure. Any doubt should be resolved through contact with your Information Governance Officer.

9. The Information Commissioner

The Information Commissioner is the body that oversees compliance with the Data Protection legislation, and has powers to force organisations to process personal data lawfully.

Where a data subject is unhappy with some aspect of the processing of their personal information they have the right to complain to the Information Commissioner.

It is recommended that any such issue should be resolved locally between the Council and the individual concerned where possible. Any request for assessment subsequently received from the Information Commissioner should be referred to the Data Protection Officer or IG Lead immediately.

10. Breaches of Data Protection

All breaches or suspected breaches of Data Protection legislation must be reported via the Information Security Incident form.

11. Responsibilities

All employees and Members and any other individual handling personal information on behalf of the Council have a responsibility to ensure that they comply with Data Protection legislation themselves and encourage others to do so.

Managers should ensure that all staff who are involved in processing personal data complete the online Information Governance training.

Particular responsibility is given to specific officers as follows:

- The Chief Operating Officer as SIRO (Senior Information Risk Officer) is responsible for ensuring that ESCC complies with Data Protection legislation.
- The County Council's Data Protection Officer is responsible for co-ordinating all Data Protection activities within the authority, helping and advising departments, monitoring compliance with the legislation and acting as the point of contact with the Office of the Information Commissioner.
- Departmental Information Governance Officers and the Customer Services Team are responsible for providing advice and guidance, ensuring registrations are kept up to date, ensuring corporate requirements are met and all relevant aspects of the legislation are complied with.

12. Contacts

Data Protection Officer

Heidi Judd	01273 482184	DPO@eastsussex.gov.uk

Departmental Information Governance Officers

ESCC IG Lead	Sarah Turner	01323 466711
Adult Social Care	Mick Acott	01273 481287
Children's Services	Peter Questier	01273 482291
Communities, Economy & Transport, Business Services Department and Governance Services	Tracey Wallace /Kathy Gardner	01273 482913

Office of the Information Commissioner

The Information Commissioners
Wycliffe House
Water Lane
Wilmslow
Cheshire SK9 5AF

website: www.ico.gov.uk