Personal Privacy Policy

Author: Robert Beane (Veritau Ltd)
Date: February 2016
Approval: Management board
Audience: Council officers and members

Policy Statement:

The council collects and holds a significant amount of personal data, of various people including residents of North Yorkshire, employees and council members. The council has a responsibility to ensure that the privacy of these people is adequately protected. This policy sets out guidance and measures to ensure the council and its officers fulfil that responsibility.

This policy recognises that whilst privacy must be protected, it is also sometimes necessary or prudent for data to be shared both internally and externally.

Purpose and Objective:

Data, including personal data, is a resource which must be effectively managed like other resources and it is subject to certain risks which must also be managed. This policy aims to guide the council in managing the personal data it holds, and in achieving the following objectives:

- Protecting the rights of data subjects; and
- Allowing the council to effectively use the personal data it holds as a resource for the delivery of its services, both to individuals and to the public as a whole.

The Data Protection Act 1998 (DPA) provides the principal legal framework which must be followed in achieving these objectives and this policy therefore incorporates the provisions of that Act. Schedule 1 to the DPA lists eight data protection principles which must be complied with when dealing with personal data. These principles are set out in Annex 2 to this policy.

This policy incorporates the council's former data protection policy and is a component of the council's overall information governance strategy. It should therefore be read in the context of that strategy.

Scope:

This policy applies to the following in relation to their capacities as data controllers and data processors on behalf of the council:

- All council employees;
- Council contractors, volunteers and other unpaid or temporary workers (for example, work experience placements);
- Elected members; and
- Registrars of births, marriages and deaths.

It does not apply to schools as they are data controllers separate from the council. Schools must therefore adopt their own policies, although they may wish to apply the same principles as set out in this policy.

This policy applies to all information and data held by the council and is not limited to personal data. The protection and disclosure of information of commercial or political significance must also be properly controlled.

Risks:

This policy aims to reduce the risks associated with the misuse of personal data, including the harm that might occur to data subjects such as customers, clients and the council's employees. It also aims to reduce any consequential financial, legal and reputational risks to the council and its members. It does so in the context of the overall information governance policy framework.

Information Asset Owners

Each corporate director must nominate an information asset owner (IAO) for each identifiable information asset. The IAO should take responsibility for their information asset and:

- Record it accurately on the directorate information asset register;
- Identify risks to that information (including risks associated with its storage and transmission) and apply appropriate mitigation; and
- Identify any personal data and ensure compliance with the Data Protection Act 1998 (DPA).

Privacy Notices

(otherwise known as fair processing notices or fair collection notices)

As part of its obligations to protect data, the council has an obligation to provide a privacy notice to those individuals about whom it collects personal data setting out how it will be used. IAOs are responsible for ensuring that this obligation is complied with in relation to the personal data their service holds. A privacy notice must:

- Identify the council as the data controller;
- Provide a relevant point of contact within the council;
- Identify the purpose(s) for which the personal data is being processed. The purpose(s) can be drawn from the council's notification to the information commissioner; and
- Provide brief details of how the data will be processed, in particular detailing anything that a reasonable person might not expect to happen to their personal data, for example if the data is to be disclosed to an external body.

A privacy notice need not be in writing although this is preferred as it provides evidence of the notice being provided. It may sometimes be easiest to include a few paragraphs detailing all the required privacy notice information in other written material provided to the individual at the time the data is collected.

The information governance manager must ensure that the council's public website contains a statement describing how personal data collected and held by the council will be managed. Service level privacy notices can refer to this statement in order to be kept short but should still contain all the details of the intended processing which are specific to that service.

Open Data and Social Media

A separate policy covers the use of personal data obtained from open sources and social media.

Data Processing by Contractors

The council will sometimes have data processed by another body which in certain circumstances may be acting as a 'data processor' for the council. If so, the council is legally liable for any breaches of the DPA by the data processor. Contractors may also become data controllers in their own right or be both a data controller and a data processor for different aspects of a single contract. The council's contracts with third parties must therefore make provision for the protection of the privacy and information rights of the council's customers, clients and employees. This will reduce any risk to the council relating to the incorrect processing of personal data by the third party.

Standard contract clauses for data processors can be found in annex 1 to this policy.

The council's nominated contract officers will assess potential suppliers for their suitability to carry out the work required. In addition to the usual checks for technical competence and financial stability, confirmation of the following will be required:

- That the contractor has the necessary security measures to protect the data and that these measure are operational;
- That the contractor's own data policy framework is adequate; and
- That the contractor's staff are appropriately and adequately trained in relation to the use and handling of the data.

Where appropriate, contracts should also include a right of audit allowing the council to inspect the contractor (including its premises and systems) and confirm that information risks are being appropriately managed.

This assessment applies to all arrangements, including formal contracts, partnership agreements and collaborative arrangements with other bodies which lead to any personal data held by the council being processed on its behalf by another body.

The policy applies when the council:

- Needs to share personal data it already holds with an external body to deliver a service; or
- Intends to contract with an external body for that body to collect and process personal data in order to deliver a service to the council or on its behalf.

Data Sharing

The council should maintain appropriate arrangements for both ad hoc and routine data sharing with external bodies. Although data sharing is a reciprocal process, this policy is more concerned with the disclosure of personal data by the council. However, IAOs should note that the collection of personal data from another data controller must also be:

- Fair;
- Necessary for the purpose(s) for which it is collected; and
- Not excessive for that purpose.

IAOs and data users should be aware of the information commissioner's statutory 'data sharing code of practice' and the multi-agency information sharing protocol.

Where repeated or routine data sharing with external bodies is taking place this should be codified in an agreement with the other party or parties. The council, in partnership with other agencies, has developed and agreed the multi-agency information sharing protocol. This protocol has been developed to ensure that information is being shared lawfully, appropriately and in compliance with best practice. The protocol aims to establish consistent principles and practices to govern the sharing of personal and non-personal information within and between partner agencies. The ethos of the protocol is for partner agencies to share information in all situations to improve service delivery and resident outcomes and to support safeguarding, except where it would be unlawful to do so.

A template data sharing 'arrangement' with guidance on how it should be completed can be found annexed to the protocol. Further advice and guidance in relation to the use of the template should be obtained by contacting the information governance manager or the relevant DIGC.

Data sharing agreements drafted and proposed by another party must only be entered into or agreed after considering advice from the information governance manager and/or legal services.

Internal Data Sharing

The ICO code of practice also applies to internal data sharing, although it does not describe at what level of management a disclosure constitutes 'sharing' as opposed to mere processing.

New or revised processes and procedures which significantly extend the range of internal recipients of personal data should be documented by means of a privacy impact assessment (see below for further details). Any additional safeguards and controls identified by the assessment should be implemented before processing takes place.

Transferring Data

Data held by the council may need to be transferred internally between locations or from one information system to another. Data may also need to be transferred to other organisations for processing or to facilitate data sharing. Data should only be transferred using appropriate methods of transmission which take account of the need to maintain data integrity and security. Transmission includes data sent by post, email and electronic file transfer. It also includes the physical transfer of data using portable electronic devices.

Methods of data transmission and levels of protection will be kept under review by the council. The risks to data integrity and security should be evaluated by IAO's and the most appropriate method for transmission chosen.

To minimise possible risks, the following measures should be taken:

- Data must not be transferred to any country outside the European Economic Area (EEA) unless appropriate safeguards are in place;
- Secure email facilities must be used for communicating personal data (the council's policy on email can be found here);
- Full disk encryption must be enabled on any mobile electronic device; and
- Mobile electronic devices should have the facility to enable them to be remotely disabled or for the data held on them to be wiped.

Sending personal data by post is the least secure method of transmission and therefore other more secure methods should be considered. If the post is the only option available then best practice is always to double check the address, ensure it is clearly written (typed if possible) and include a senders' address on the back of the envelope. All envelopes containing personal information should be marked 'private and confidential'.

Sensitive information should be sent by special delivery, or even hand delivered, and large amounts of information might need to be double enveloped. The intended recipient should also be informed in such circumstances and confirmation of receipt obtained.

Single Ad-hoc Requests

Usually, compliance with requests for single or ad hoc disclosure will be at the discretion of the council and it will be for the person making the request to persuade the council that it is right to disclose the data. Generally, this will mean balancing the need of the person making the request against the policy objectives of the council and the information rights and privacy or confidence of the person or persons to whom the data relates. This decision should only be made by suitably trained and experienced staff of appropriate seniority (for example - head of service or assistant director). Any officer in doubt about a request for disclosure should consult the information governance manager.

In some cases, the council can be legally obliged or compelled to disclose personal data which would not otherwise be disclosed. Enquiries relying on such obligations will probably refer to the relevant legal provisions but in cases of doubt, officers should consult the information governance manager and/or legal services.

Once a request has been processed, the facts of the disclosure and the reasoning behind a decision if discretion has been applied, even for a refusal, should be recorded. The relevant case file is usually the appropriate place but a special folder for such requests may be set up if necessary.

Subject access requests in which a person asks for his or her own data, and the disclosure of personal data in FOI and EIR requests, are dealt with in the information access policy.

Privacy Impact Assessments

A privacy impact assessment (PIA) is a way to foresee possible risks to individual privacy when changes to services, systems or procedures are proposed, or where data sharing is being considered.

The council should therefore consider privacy issues as part of the planning stage for any change programme or project, or before data is shared with an external partner where it is anticipated that the data sharing will take place on a regular basis. A PIA should be completed by anyone formally appointed as a project manager, or anyone fulfilling that role where:

- A new service is being developed;
- There is a significant change to an existing service; or
- New or revised methods of data collection are being implemented.

Similarly, a PIA should be completed by the relevant IAO where data sharing is being considered which is significant in nature or likely to be repeated on a regular basis. A PIA not required where the partner organisation is a signatory to the multi-agency information sharing protocol as this provides a suitable framework for managing the risks to individual privacy.

A series of screening questions should be answered before completing the PIA.

Further advice including examples of completed privacy impact assessments can be obtained from the information governance manager.

Complaints

It is recognised that there is often an overlap between the council's corporate complaints policy and data privacy matters. A complaint by a person that his or her data protection rights have been breached may also result in an investigation into a data security incident. For example, a report that personal data has been published or disclosed without the consent of the complainant might indicate a failing in the council's data security procedures. Similarly an investigation into a data security incident may lead to a data subject being informed of an incident of which he or she was previously unaware, and he or she then makes a complaint.

Both the data security incident reporting procedure and the complaints procedure may therefore be activated. In such circumstances, officers should be aware of both procedures, ensure that they are cross-referenced, and that the outcomes of both (a satisfied customer, and remedial action to address any data security issues) are achieved.

For complaints about subject access requests, FOI and EIR requests see the information access policy.

Compliance

All officers of the council are required to comply with this policy in respect of all of its provisions and ethos. Failure to do so may be regarded as a breach of the officers' code of conduct and could result in disciplinary action being taken against the member of staff concerned.

Advice

For advice on this policy, contact the information governance manager (Veritau) or legal services.

Governance

Responsible officer	Information governance manager
Accountable officer	Senior information risk owner (SIRO)
Consulted	CIGG
Informed	Information asset owners

Review and Revision

This policy will be reviewed by the information governance manager annually. Any proposed changes to the policy will be considered by the corporate information governance group which is chaired by the SIRO.

This policy is a revision of the data protection policy version 1. It incorporates the following policies:

- Charges for information
- Fair processing notices
- Data sharing with partners
- Data processing by contractors
- Security classification

References

This policy should be read in the context of the council's other policies and guidelines in addition to national legislation, codes of practice and accepted best practice. In particular, this policy should be read in the context of:

- The Data Protection Act 1998
- The ICO's data sharing code of practice
- Multi-agency information sharing protocol
- The ICO's privacy notices code of practice
- The Cabinet Office government security classifications

The following council strategies and policies are directly relevant to this policy:

- Information governance policy
- Information access policy
- Technical security policy
- Document and records management policy

The following council documents are subject to this policy. Readers should have regard to this policy in applying them. In the event of a contradiction, this policy takes precedence:

- Data protection guidelines and procedures fair processing notice template;
- Guidance on the consideration and use of CCTV; and
- Procedure and appeals under the Data Protection Act 1998.

North Yorkshire County Council

Key Messages

1. The Data Protection Act 1998 (DPA) governs the protection of personal privacy by the council.
2. It is necessary to balance the need for information sharing at the same time as maintaining personal privacy for individuals.
3. Information asset owners (IAOs) are responsible for the personal data held within their information asset (IA).
4. IAOs are responsible for providing privacy notices detailing how an individual's data will be processed.
5. Data processing by an external body is subject to specific obligations, and any contracts with third parties should make provisions for safeguarding privacy.
6. The multi agency information sharing protocol governs information sharing with our partner agencies.
7. Technical measures such as secure email or encryption are necessary in order to transmit data securely.
8. A privacy impact assessment (PIA) should be carried out by the relevant project manager where changes to systems or procedures are proposed, or where data sharing is being considered. The PIA will help the project manager screen any potential risks to individual privacy and explain how they will mitigate them.

Annex One: Standard Clauses for Data Processing Contracts

Data Protection Act 1998 standard clauses for data processing

Definitions:

"The Act": The Data Protection Act 1998
"Personal data": as defined in the Act, and which is supplied to or processed by the provider on behalf of the council.
"The provider": the contractor which will process the personal data
"the council": North Yorkshire County Council

1.0 Protection of personal data

1.1 North Yorkshire County Council is the data controller of the personal data and the provider is a data processor under the terms of the Act. The provider will not process the personal data except for the purpose of or in accordance with this contract.

1.2 The provider shall maintain appropriate technical and organisational security measures and in particular shall:

1.2.1 secure personal data against unauthorised disclosure or accidental loss or corruption by such technical and managerial controls as would be appropriate if the provider was the data controller.

1.2.2 hold the personal data for only as long as necessary for the completion of the contract and then destroy it or return it to the council in a secure manner.

1.2.3 not retain the personal data or any copy of it.

1.3 The provider shall ensure the conformity of any of its staff or agents who have access to the personal data to the above requirements. The provider will ensure that such employees and agents receive appropriate data protection training and understand their responsibilities under the Act in respect of personal data.

1.4 Should the provider receive a subject request for personal data it will be referred to the information governance officer of the council as soon as practicable after receipt.

1.5 Should the provider sub-contract any part of the services in accordance with the contract then the provider shall ensure that any sub-contract or other arrangement with any such sub-contractor shall include a binding legal obligation upon the sub-contractor to comply with the obligations set out in this clause. For the avoidance of doubt any such sub-contracting shall not relieve the provider of its obligation to comply fully with this clause.

1.6 The provider shall be liable for and shall fully indemnify the council against all claims, demands, actions, costs, proceedings and liabilities of any sort that the council incurs due to the provider's or any sub-contractor's breach of this clause.

1.7 The provider shall provide to the council on request evidence to the council's reasonable satisfaction that it can comply with this clause.

1.8 The obligations set out in this clause shall remain enforced notwithstanding termination of this agreement.

Annex Two: Data Protection Principles

The Data Protection Act (DPA) provides the principal legal framework which must be followed in achieving these objectives and this policy therefore incorporates the provisions of that Act. Schedule 1 to the DPA lists eight data protection principles which must be complied with when dealing with personal data.

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless;

(a) at least one of the conditions in schedule 2 is met, and
(b) in the case of sensitive personal data, at least one of the conditions in schedule 3 is also met.

2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

4. Personal data shall be accurate and, where necessary, kept up to date.

5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

6. Personal data shall be processed in accordance with the rights of data subjects under this Act.

7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

North Yorkshire
County Council