Peterborough City Council

Data Protection Policy

Growing the right way for a bigger, better Peterborough

Document Control:

Purpose of document:	To provide a framework for the council to comply with the Data Protection Act 1998
Intended audience:	Everyone who holds or uses information held by, or on behalf of, Peterborough City Council.
Type of document:	Policy
Document lead/author	Ben Stevenson, Corporate Information Governance Manager
Other documents that link to this one:	All documents posted on the Information Governance page of Insite.
Document ratified/approved by:	Audit Committee
Version number:	Version 1.1
Issue date:	March 2016
Dissemination method:	Notification to staff via the *Weekly Round-up* newsletter and via *All Staff* notifications on the front page of Insite.
Date due for review:	Annually April
Reviewer:	Information Governance

DOCUMENT REVISION RECORD:

Description of amendments:	**Version No.**	**Date of re-approval and re-issue**
Document Control page added. Minor sense check amendments throughout.	1.1	
Addition of Appendix 2 Confidentiality Agreement	1.1	
Additions of consequences for staff, points of contact and do's and don'ts	1.1	

CONTACT:
This document has been produced by the Governance Team. Any comments or queries regarding the content of the document should be referred to: **foi@peterborough.gov.uk**

Contents

Introduction 5
Purpose 5
Scope 6
The Policy 6
Data Protection Principles 7
Key definitions in the context of this policy 8
Data Controller 8
Data Processor 8
Data Controller-Data Processor Relationship 8
Personal Information 8
Sensitive Personal Information 9
Data Breaches 9
Consequences of data breaches 10
The Sharing of Personal Information 10
Anonymisation 11
Pseudonymisation 11
Information sharing agreements 11
Privacy Impact Assessments 12
Roles and Responsibilities 12
Chief Executive 12
Senior Information Risk Owner (SIRO) 12
Information Governance Group 13
Information Governance Team 13
Caldicott Guardians 13
Responsibilities of Each Directorate / Information Asset Owners 14
Responsibilities of Managers 14
Responsibilities of Staff – all staff (permanent and temporary) 15
Responsibilities of staff – additional instructions for temporary staff 15
Responsibilities of Members 16

Subject Access Requests 16
Policy Review 16
Monitoring Compliance 16
Training 17
Appendix 1 The Do's and Don'ts of Data Protection 18
Appendix 2 19
Reasons/purposes for processing information 19
Type/Classes of information processed 20
Who information is processed about 20
Appendix 3 .....
Confidentiality Agreement 22

Introduction

Peterborough City Council needs to collect and use different types of information about people with whom it deals and communicates with in order to operate. These include current, past and prospective employees, contractors, suppliers, service users and carers. In addition, it may occasionally be required by law to collect and use certain types of information to comply with the requirements of government departments for business data.

The Data Protection Act 1998 details the requirements and safeguards which must be applied to personal data to ensure the rights and freedoms of living individuals are not compromised. The Act stipulates that those who record and use personal information must be open about how the information is used and must follow good information handling practices. It applies to the collection, use, disclosure, retention and destruction of data.

It is Peterborough City Council's obligation, as Data Controller, to ensure compliance with the Data Protection Act 1998. This policy applies to all personal data held by the Council and includes manual/paper records and personal data that is electronically processed by computer systems or other means such as CCTV systems.

Purpose

The purpose of this policy is to enable Peterborough City Council to

- Comply with the law in respect of the data it holds about individuals
- Protect the Council's customers, service users, staff and other individuals
- Protect the organisation from consequences of a breach of its responsibilities.
- Follow good practice

This policy will provide a framework within the Council to ensure compliance with the Data Protection Act 1998 and associated legislation relating to personal information. It should be read in conjunction with

- Information Governance Policy
- Data Incident Reporting Policy

- Freedom of Information Policy
- Records Retention Policy
- Disciplinary Policy
- Whistleblowing
- ICT policy

Peterborough City Council recognises its responsibility to fully implement its duties in respect of the Data Protection Act and to ensure that all of its employees and suppliers understand and can implement all of the requirements of the Act.

This policy will underpin any operational processes and procedures connected with the eight principles of the Act.

Scope

This policy will apply to anyone accessing or using Council held personal information, including for example: employees, temporary or contract staff, volunteers, work placements, council members, contractors, suppliers, services providers or other partners or agencies.

Peterborough City Council requires that all third parties acting as Data Processors will comply with the terms of this and other related Information Governance policies.

The Policy

This policy is a key policy in the Information Governance Framework. Implementation and monitoring will follow the processes set out in the Information Governance Policy.

The Council will:-

- Observe fully, conditions regarding the fair collection and use of personal information
- Meet its legal obligations to specify the purpose for which information is used
- Collect and process appropriate information and only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements

- Ensure the quality of information used
- Apply strict checks to determine the length of time information is held
- Take appropriate technical and organisational security measures to safeguard personal information
- Ensure that personal information is not transferred abroad without suitable safeguards
- Ensure that the rights of people about whom the information is held can be fully exercised under the Act.

In addition the Council will ensure that:-

- There is someone with specific responsibility for data protection in the organisation
- Everyone managing and handling personal information understands that they are contractually responsible for following good data protection practice;
- Everyone managing and handling personal information is appropriately trained to do so
- Everyone managing and handling personal information is appropriately supervised
- Queries about handling personal information are promptly and courteously dealt with
- Methods of handling personal information are regularly assessed and evaluated
- Guidance is in place for robust governance of sharing data with Partners and third parties

Data Protection Principles

There are eight Data Protection Principles in the Act that the Council must comply with in relation to personal information. In summary these are that personal information will be:-

1. Processed fairly and lawfully
2. Obtained only for one or more specified and lawful purposes and not processed in a manner incompatible with that purpose
3. Adequate, relevant and not excessive
4. Accurate and where necessary, kept up to date

5. Not be kept for longer than is necessary
6. Processed in accordance with the rights of the data subjects
7. Protected by appropriate technical and organisational
8. Not transferred to a country or territory outside the European Economic Area without adequate protection

Key definitions in the context of this policy

Data Controller

The Council is the data controller and is ultimately responsible for ensuring compliance with the Data Protection Act 1998. The Council has two registrations with the ICO; one listing the uses as shown in Appendix 1 and the second is for electoral register due to the Chief Executive's role as Electoral Registration Officer.

Data Processor

A data processor is the person/service who process personal data in line with the list of uses permitted by the Council's data protection registration. A data processor does not own the data and cannot use it for purposes other than stated in the contract or where a legal gateway exists. Any use or sharing of data should not be done without the written consent of the data controller.

Data Controller-Data Processor Relationship

Where the controller and processor are not the same i.e. the council and a partner agency, the relationship must be underpinned by a contract. When commissioning an external party to provide a service to the council where personal data is to be processed, officers must ensure that a contract is drawn up and contains the appropriate detailed schedules of the data to be processed as well as the clauses regarding the arrangements for the use, storage, retention and deletion of data by that external party. In all cases, Legal Services will review every contract and ensure that it meets requirements.

Personal Information

The ICO define personal information as information relating to a living individual who can be identified from that information. It may also be possible

to identify an individual from that and other information which is in the possession of, or likely to come into the possession of the Council. It also includes any expression of opinion about the individual and any indication of the intentions of the Council or any other person in respect of the individual.

It is important to note that, where the ability to identify an individual depends partly on the information held and partly on other information (not necessarily data), the information held will still be personal.

Sensitive Personal Information

Sensitive personal data means personal data consisting of information as to -

- the racial or ethnic origin of the data subject,
- his/her political opinions,
- his/her religious beliefs or other beliefs of a similar nature,
- whether he/she is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992),
- his/her physical or mental health or condition,
- his/her sexual life,
- the commission or alleged commission by him/her of any offence,
- any proceedings for any offence committed or alleged to have been committed by him/her, the disposal of such proceedings or the sentence of any court in such proceedings.
- Credit card/debit card details pertaining to the data subject

Data Breaches

Peterborough City Council holds large amounts of data and information; this can include personal and sensitive information but also, for example, commercially sensitive information or simply data. Every care is taken to avoid a data protection breach by protecting personal information and also by taking steps to avoid losing any Council data. In the unlikely event of data being lost or shared inappropriately, it is vital that appropriate action is taken to minimise any associated risk as soon as possible. The Data Incident Reporting Policy covers the process. You should report any breaches, suspected and

confirmed, to the Information Governance service. Guidance can be found the process in the Data Incident Reporting Policy.

Breaches will be risk assessed based on the following criteria

- The potential harm to the data subject as a result of the breach, including any distress the data subject may suffer as a result of the breach, which is dependent on the volume and the sensitivity of the data involved.
- The volume of the data involved – this must be determined by the facts and extent of the breach.
- The sensitivity of the data involved – where the data is classed as sensitive personal data as defined by section 2 of the Data Protection Act 1998 and the release of that data can lead to the data subject suffering substantial harm.

The Information Governance service will retain a centralised record of breaches to ensure consistency and visibility.

Consequences of data breaches

The consequences can be that the individual data subject can suffer mentally, physically or financially. Aside from the impact elsewhere, it is the individual data subject who should be at the heart of our concern.

A data breach can cause loss of reputation for the council and a loss of confidence in our ability to provide a service. It may be reported in the media or appear on social media.

The Information Commissioner can fine the authority up to £500,000 or force the Chief Executive to sign an undertaking to improve, or undertake an audit of the authority and our practices.

Employees can also face personal legal action including criminal prosecution for acting outside this policy and the Data Protection Act.

The Sharing of Personal Information

In line with the Information Commissioner's guidance and the Information Sharing Procedure, it is the Council's stated policy that personal information can only be shared where a legal gateway exists or consent has been obtained. Personal information cannot be used by the Council for the planning of service provision. This also means that personal information cannot be shared with

partners for this purpose or where a partner may process data on our behalf, they may not use personal information without the written consent of the Council.

The sharing of personal information must be by secure means such as GCSX email or Box. Secure file sharing may also be used with agreement from Information Governance and ICT. This will be in line with the ICT Policy.

Failure to comply with this policy will result in the appropriate action being taken under either the relevant policy or contract.

It is also important to note that information to identify a living person is not limited to names and full addresses. Mapping point data can also potentially identify a person as can limiting the address to post code.

Anonymisation

Data can be anonymised i.e. removal of information which could lead to the identification of an individual and shared with partners. Where five or less individuals share the same characteristics then these should also be removed. Please seek advice from the Head of Performance & Informatics before attempting such work.

Pseudonymisation

Where it is not necessary to share personal data but anonymised is not sufficient, then consideration should be given to the pseudonymising approach. This means when information is supplied it is not identifiable to the user but the individual producing the information has a "key" to identify. Further guidance can be obtained from the Head of Performance & Informatics.

Information sharing agreements

Any sharing of personal information between the Council and other organisations will be subject to an information sharing protocol that commits the partners to an agreed data transfer process that meets the requirements of the Data Protection Act, and as specified by an overarching Information Sharing Protocol.

It should be noted that this includes Partner organisations such as Serco, Vivacity and Enterprise. Whilst the partner organisation may process data on behalf of the Council, the Council remains the data controller.

Further guidance on the completion of Information Sharing Agreements is contained within the Information Sharing & Open Data Guidance or can be obtained from the Information Governance service.

Should you enter into an information sharing agreement, you must provide a copy of the agreement to the Information Governance service prior to the information being shared.

Privacy Impact Assessments

A privacy impact assessment will be carried out whenever there are projects, new or changed service activities, or new ICT that could potentially impact on the privacy of individuals. The results of assessments will be reported to the Information Governance Group. Guidance can be sought from the Privacy Impact Assessment Procedure.

Roles and Responsibilities

Chief Executive

The Chief Executive has overall accountability and responsibility for all aspects of information governance, including data protection.

The Chief Executive is required to provide assurance that all risks to the Council relating to data protection and information security are effectively managed and mitigated.

The Chief Executive will delegate responsibility for compliance with the Data Protection Act (including the implementation of this policy and other related policies) to the Senior Information Risk Owner.

Senior Information Risk Owner (SIRO)

As SIRO, the Director of Governance will lead and foster a culture that values, protects and uses information for the benefit of both the authority and its customers. The SIRO has overall responsibility in ensuring that information threats and data security breaches are identified, assessed and any data breaches managed.

The SIRO will ensure that the Chief Executive and the Strategic Governance Board are fully briefed on all information risk issues to the authority.

Information Governance Group

It is the role of the Information Governance Group to define the organisational policy in respect of data protection taking into account any legal and local authority requirements and to report findings to the Strategic Governance Board.

The Information Governance Group is also responsible for ensuring that the Council's approach is:

- co-ordinated to provide a corporate approach to compliance
- effective in terms of resource, commitment and execution
- appropriately communicated to staff.

Information Governance Team

The Corporate Information Governance Manager and Access to Information Manager will act as point of contact for all data protection issues, including access requests, and will be the first point of contact for all requests for personal information.

The Information Specialist is also responsible for ensuring that the Council is registered with the Information Commissioner's Office for data processing, that the registration accurately reflects the data processing activities undertaken by the Council and that the registration is maintained and renewed as required.

Caldicott Guardians

The Caldicott Guardians for Social Care are responsible for the safeguarding of information processed for social care work and will oversee all procedures for protecting the confidentiality of service user information and enabling the appropriate information sharing.

The Caldicott Guardians will ensure that compliance with this policy is achieved and will work proactively (supported by nominated staff) to ensure that

personal data processed for social care is appropriately safeguarded to meet the requirements of the Data Protection Act 1998, and other relevant legislation.

The Caldicott Guardians will provide advice, guidance and expertise to the Information Governance Group in relation to social care service user information and will support the Information Governance structures in place within the Council.

The Caldicott Guardian is currently Kim Sawyer, Director of Governance.

Responsibilities of Each Directorate / Information Asset Owners

Each directorate will designate an Information Asset Owner (IAO) to take responsibility for the correct protection and handling arrangements for the information assets 'owned' by them. The IAO will be part of the Information Governance Group.

Where the processing of personal information is quite complex - for example - in relation to health and social care, directorates should draw up specific data protection guidance for their directorate which is aligned with, and supports, this policy. This may include specific operational procedures, including directorate induction and training, to ensure that detailed data protection practice is established and followed.

Responsibilities of Managers

All managers are required to ensure that they (and their staff) understand and adhere to this policy and any associated procedures. They are responsible for ensuring that staff are informed and updated on any changes made to this policy.

All managers must identify and report any risks or breaches to the security of personal data processed by the Council to their relevant line manager or appropriate Information Asset Owner.

All managers must ensure that their staff undertake information governance training and any training in data protection/information security which is specific to their role. Refresher training will be undertaken annually.

Responsibilities of Staff – all staff (permanent and temporary)

All staff, whether permanent or temporary, are required to read, understand and accept any policies and procedures that relate to personal data that they may handle in the course of their work.

All staff have a responsibility for data protection and are required to adhere to this policy, any associated procedures and to attend any associated training.

All staff must:

- Understand the main concepts within the Data Protection legislation; the eight principles, sensitive data and informed consent.
- Identify and report any risks to the security of personal data processed by the Council to their line manager or the Information Asset Owner.
- Assist their customers/service users to understand their rights and the Council's responsibilities in regards to data protection.
- Identify and report any subject access requests to the Data Protection Lead (or directorate Information Governance Lead if there is one designated) so that they can be processed in accordance with the Data Protection Act.

Responsibilities of staff – additional instructions for temporary staff

It is a requirement of Peterborough City Council that all temporary staff, agency staff, volunteers, work placement students and all managers requesting access to systems for these temporary workers, should read, and undertake to comply with these compliance guidelines in accordance with the Data Protection Act 1998 and the council's Data Protection Policy.

In addition, all staff on temporary contracts, agency staff, volunteers and work placement students, and their line managers, are required to read and sign the Confidentiality Agreement at Appendix 2 of this document **before** access to any systems containing person identifiable information is granted.

Responsibilities of Members

All Peterborough City Council elected Members are registered as Data Controllers in their own right and when considering the use of personal information for any particular purpose, they should take into account the context in which that information was collected to decide whether their use of the information will be fair and lawful.

Further information for Members is available via the Director of Governance or can be accessed on the Information Commissioner's website in a document entitled "Advice for the elected and prospective members of local authorities".

Members should also refer to council's "Members' Code of Conduct", which is intended to promote high standards of behaviour amongst the elected and co-opted members of the council and which is available on the council's website.

Subject Access Requests

Any person whose details are held / processed by the council has a general right to receive a copy of their own information. There are a few exceptions to this rule, such as data held for child protection or crime detection / prevention purposes, but most individuals will be able to have a copy of the data held on them.

All such requests should be referred to the Information Specialist to respond to. Individual officers should not seek to respond to any request. The Subject Access Procedure will be adhered to.

The ICO guidance on handling subject access requests (SAR) can be found here.

Policy Review

A review of this policy will take place annually to take account of any new or changed legislation, regulations or business practices.

Monitoring Compliance

Compliance with this policy and related standards and guidance will be monitored as part of the work of the Information Governance Group. Findings will be reported to the Strategic Governance Board.

Breaches will be reported in line with the Data Incident Response Policy. The Information Governance team will maintain a central record and will ensure that the Council responds in accordance with its policies.

Information Governance will form part of risk based audit plan for the Council. Audits can be undertaken by Internal Audit with the support of the Information Governance service.

As part of the monitoring and evaluation, an action plan for improvements in Data Protection practices will be formulated as required by the Information Governance Group.

Disregard for this policy by employees may be treated as misconduct and a serious breach may be treated as gross misconduct and lead to dismissal. In the case of contractors, partner representatives, agency workers and volunteers, disregard of this policy may be grounds for termination of that relationship with the Council. Disregard for this policy by Members may be regarded as a breach of the Members' Code of Conduct and referred to the Monitoring Officer.

The Act creates a number of criminal offences and failure to comply with the requirements of the Act could result in a fine of up to £5,000 in a Magistrates court or an unlimited fine in a Crown court.

Training

The Information Governance Team will lead on the development of mandatory training either through e-learning modules or face to face. The training will be developed through the Information Governance Group and agreed by the Corporate Management Team (CMT).

Training on specific data security measures such as Box and GCSX will be mandatory for staff, or partner staff, who are required by the council to use such measures.

Appendix 1 The Do's and Don'ts of Data Protection

Do's

Do check that you have consent to share data

Do check that you have an information sharing agreement in place

Do think about data as it were about you

Do only hold data for as long as it is needed

Do destroy files correctly and confidentially

Do make sure you have correct and accurate data

Don'ts

Do not share your passwords

Do not leave your PC unlocked when away from your desk

Do not leave documents on your desk if they contain personal or sensitive information

Do not disclose personal information unless you are sure you can and you know who is asking for it

Appendix 2

Reasons/purposes for processing information

We process personal information to enable us to provide a range of government services to local people and businesses which include:

- maintaining our own accounts and records
- supporting and managing our employees
- promoting the services we provide
- marketing our local tourism
- carrying out health and public awareness campaigns
- managing our property
- providing leisure and cultural services
- provision of education
- carrying out surveys
- administering the assessment and collection of taxes and other revenue including benefits and grants
- licensing and regulatory activities
- local fraud initiatives
- the provision of social services
- crime prevention and prosecution offenders including the use of CCTV
- corporate administration and all activities we are required to carry out as a data controller and public authority
- undertaking research
- the provision of all commercial services including the administration and enforcement of parking regulations and restrictions
- the provision of all non-commercial activities including refuse collections from residential properties,
- internal financial support and corporate functions
- managing archived records for historical and research reasons
- data matching under local and national fraud initiatives
- we also process personal information to enable us to design, test and demonstrate software to assist service delivery

Type/Classes of information processed

We process information relevant to the above reasons/purposes which may include:

- personal details
- family details
- lifestyle and social circumstances
- goods and services
- financial details
- employment and education details
- housing needs
- visual images, personal appearance and behaviour
- licenses or permits held
- student and pupil records
- business activities
- case file information

We also process sensitive classes of information that may include:

- physical or mental health details
- racial or ethnic origin
- trade union membership
- political affiliation
- political opinions
- offences (including alleged offences)
- religious or other beliefs of a similar nature
- criminal proceedings, outcomes and sentences

Who information is processed about

We process personal information about:

- customers
- suppliers
- staff, persons contracted to provide a service
- claimants
- complainants, enquirers or their representatives
- professional advisers and consultants

- students and pupils
- carers or representatives
- landlords
- recipients of benefits
- witnesses
- offenders and suspected offenders
- license and permit holders
- traders and others subject to inspection
- people captured by CCTV images
- representatives of other organisations

Appendix 3

PETERBOROUGH CITY COUNCIL

Confidentiality Agreement

Temporary Staff, Agency Staff, Volunteers and Work Placement Students

It is a requirement of Peterborough City Council that all temporary staff, agency staff, volunteers, work placement students and all Managers requesting access to systems for these temporary workers, should read, and undertake to comply with, these compliance guidelines in accordance with the Data Protection Act 1998 and the council's Data Protection Policy.

1. **General Principles**

1.1 It is the responsibility of all Managers and Supervisors of temporary staff, agency staff, volunteers and work placement students who have access to personal information (including sensitive personal information) to ensure that these workers are aware of the need for confidentiality under the Data Protection Act 1998. Managers and Supervisors must make temporary staff, agency staff, volunteers and work placement students aware of the Good Practice Guidelines below that must be followed during the handling of all personal information.

1.2 Users of council services and members of staff are entitled to assume that any personal information which is collected or recorded during the course of their involvement with the organisation will not be disclosed inappropriately by any person or persons working within the organisation.

1.3 All temporary staff, agency staff, volunteers and work placement students hired by the council are in a position of trust. Any abuse of this trust will be construed as gross misconduct and may result in legal action.

2. **Good Practice Guidelines**

2.1 Caution should be exercised in dealing with telephone requests for personal information. Temporary staff, agency staff, volunteers and work placement students should refer such requests to their Manager or Supervisor if there is any doubt about the identity of the caller.

2.2 Desks should be kept clear of paper containing personal information unless the work is actually in progress.

2.3 All papers containing personal information should be locked away in a filing cabinet or desk that is in a secure area away from public access, at the end of each working day (or when the worker leaves the office if sooner).

2.4 All service user/customer and staff records must be properly supervised or locked away when unsupervised.

2.5 All scrap paper containing personal information should be disposed of carefully in the official confidential shredding bins or other secure shredding facilities.

2.6 When working on personal information held on electronic systems, the temporary worker must ensure that:

- They do not attach or link any personal I.T. equipment or other I.T. equipment not owned by Peterborough City Council to the Council's I.T. network.
- The computer screen is locked before leaving the workstation even for a short period of time.
- Any open files are closed down and the user logs out of the network if the workstation is to be left for longer periods.
- If working remotely the worker must only use encrypted laptops or encrypted recordable media issued by the Council which must be used in line with relevant I.T. policies.

2.7 Any personal information gained during the course of temporary/agency employment, volunteer work or student work placements must not be discussed with anyone, either inside or outside the workplace, unless specifically requested to do so by the line Manager or Supervisor in the course of their duties.

To the temporary worker, agency worker, volunteer or work placement student:

Your signature on this statement will explicitly acknowledge that you undertake to comply with these guidelines.

I have read and understood the Confidentiality Agreement and accept the terms and conditions stated therein.

Signature: ……..…..

Date: ……..……

Full Name (print): ……..

Employed as: ……..…….

Employment Agency/School/College: ……

To the Manager / Supervisor:

Your signature on this statement will explicitly acknowledge that you undertake to comply with these guidelines.

I understand that I take responsibility for ensuring that the above worker is aware of, and abides by, these guidelines and confirm that they will only be granted access to personal information which is necessary to allow them to fulfil their contract or agreed duties.

Signature: ……..……..

Date: ……

Full Name (print): ……..

Team or Service: ……..……..

Location: ……

To the Manager / Supervisor:

Please ensure:

- You retain the original completed and signed copy of this form on the worker's file for the recommended retention period of 6 years after the person leaves the organisation.
- You give a photocopy of the original (signed by both parties) to the worker named above for their own records.