Agenda Item 6

Policy & Resources Committee - 8 October 2018

Data Protection Policy

Purpose of report

The report introduces the new Data Protection Policy for approval by Committee and implementation. The Policy has been revised in the light of the General Data Protection Regulations and Data Protection Act which both were introduced earlier this year.

Attachments:

Appendix 1: Data Protection Policy

Appendix 2: Initial Privacy Impact Assessment

Appendix 3: Initial Equalities Impact Assessment

1.0 Background

1.1 On 25 May 2018 and 23 May 2018 respectively, the UK saw the introduction of the General Data Protection Regulation (Europe wide legislation) and the new Data Protection Act 2018 to replace the Data Protection Act 1998. Both pieces of legislation introduce new requirements on organisations, and specifically public authorities, who process personal data and give individuals enhanced rights over their own personal data.

1.2 In response to the new legislation the Council have appointed a Data Protection Officer who has reviewed the current policies and procedures in relation to Data Protection, Information Management and Security and has recommended, as part of the council's GDPR/DPA 2018 preparations, a revised Data Protection Policy.

1.3 Previously the Council incorporated the Data Protection Policy requirements into the Information (ICT) Security Policy. After discussion with the Data Protection Officer, Monitoring Officer and Head of Resources, it is proposed that the Data Protection Policy should not form part of the ICT Security Policies but should be a stand alone policy in recognition of the fact that Data protection is a Council wide responsibility that involves more that just ICT considerations.

2.0 Key Changes

2.2 The key changes are:

- Paragraph 4.2 – Reference to the Information Asset Register
- Paragraph 4.3 Reference to the role of the Data Protection Officer
- Paragraph 4.4 A requirement for mandatory data protection training for all staff and councillors
- Paragraph 4.6 – Updated list of data subject rights and information on how to access them

- Paragraph 4.8 – revised data breech reporting requirements
- Paragraph 4.10 – inclusion of additional categories of biometric and genetic information categories. Although these are now recognised in the legislation they are unlikely to be processed by this council.
- Paragraph 4.13 -Reinforcement of privacy by design approach

3.0 Important issues to consider

3.1 Consideration has been given to both Equalities and Privacy impacts of the revised policy and initial assessments have been included at Appendix 2 and 3.

4.0 Equality and Diversity Implications

4.1 An initial Equality Impact has been carried out and all equality and diversity implications are neutral. Neither a positive nor a negative impact has been identified. The initial Equality Impact Assessment can be accessed as a background document.

5.0 Privacy Impact Implications

5.1 An initial Privacy Impact Assessment has been carried out and there are no negative privacy implications from the introduction of this revised policy.

6.0 Legal Implications

6.1 The revised policy is required to ensure we meet the requirements of the new data protection legislation.

7.0 Risk Management

7.1 There are currently three risks on the council's corporate risk registers relating to the appropriate use of personal data by staff and councillors. The implementation of this new policy will help to mitigate these risks. (RM/ICT 007 Inappropriate sharing of personal data with/between councillors; RM CORP 016 Inappropriate use of IT by staff RM CORP 017 Inappropriate use of IT by councillors)

8.0 Resource and Financial Implications

8.1 There are no known additional resource or financial implications arising from the revisions to this policy over and above those already required to meet the requirements of GDPR/DPA 2018

9.0 Constitutional Implications

9.1 Changes to the Constitution in the light of GDPR/DPA 2018 have been presented to the October 2017 Council.

10.0 Implications for our Customers

10.1 The policy supported by the Council's updated privacy statement show the Council's clear commitment to the protection of the personal data it holds, whether relating to the data of their staff or customers and should support public confidence in the Council.

11.0 Corporate Outcomes

11.1 The adoption of the new Data Protection Policy will contribute to the effective management corporate outcome by ensuring we comply with the relevant data protection legislation.

12.0 Recommendation

12.1 The Committee is recommended to consider all implications and approve the Data Protection Policy.

(Reason: To ensure compliance with current data protection legislation.)

<table>
<tr><td rowspan="2">Legal</td><td colspan="5">Power: Data Protection Act 2018/General Data Protection Legislation</td></tr>
<tr><td colspan="5">Other considerations: ICO best practice guidance</td></tr>
<tr><td colspan="6">Background Papers:</td></tr>
<tr><td colspan="6">Person Originating Report: Kirsty Squires, Data Protection Officer
☎ 01832 742999 ✉ ksquires@east-northamptonshire.gov.uk</td></tr>
<tr><td colspan="6">Date: 18/09/18</td></tr>
<tr><td>CFO</td><td>  </td><td>MO</td><td></td><td>CX</td><td></td></tr>
</table>

East Northamptonshire Council

Data Protection Policy

2018

If you would like to receive this publication in an alternative format (for example, large print, braille or audio) please contact us on 01832 742000.

Document Version Control

Author (Post holder title)	Kirsty Squires, Data Protection Officer
Type of document	Policy
Version Number	V0.3
Document File Name	Data Protection Policy Draft V0.3
Issue date	10/09/2018
Approval date and by who (CMT / committee)	CMT on dd/mm/yy
Document held by (name/section)	Kirsty Squires, Data Protection Officer, Resources
For internal publication only or external also?	internal and external
Document stored on Council website or Eunice?	Website
Next review date	

Change History

Issue	Date	Comments
V0.1	August 2018	Submitted to CMT for approval
V0.2	September 2018	With CMT changes
V0.3	October 2018	Policy and Resources Committee for approval

NB: Draft versions 0.1 - final published versions 1.0

Consultees

Internal	External
e.g. Individual(s) / Group / Section	e.g. Stakeholders / Partners /Organisation(s)
CMT	
Policy & Resources Committee	

Distribution List

Internal	External
e.g. Individual(s) / Group / Section	e.g. Stakeholders / Partners /Organisation(s)
Middle Managers	All customers via Website
All Staff	

Links to other documents

Document	Link
Privacy Impact Assessment	PIA for Data Protection Policy 2018
Equalities Impact Assessment	EIA for Data Protection Policy 2018
Privacy Statement	Council Privacy Statement

Additional Comments to note

Policy required to show how we will meet the requirements of the new Data Protection Act 2018 and General Data Protection Regulation.

Contents

1.0 Introduction / foreword

The purpose of this document is to set out how the council will manage the lawful and fair handling of personal data in accordance with the Data Protection Act (DPA) 2018 and the General Data Protection Regulation 2016 (GDPR).

GDPR regulates the processing of personal data. Processing includes everything from the point we receive the data to the point we destroy it, including any sharing of information with other parties whether required by law or not. Personal information is information relating to an identified or identifiable living natural person, which is held either electronically or in manual form. GDPR and the DPA 2018 also give enhanced rights to individuals whose personal information is processed by organisations.

The council needs to collect and use personal information in order to carry out its functions effectively. Information can be held concerning its current, past and prospective employees, suppliers, service users, residents and others with whom the council communicates.

The council, it's processors (organisations we use to process personal data on our behalf) and, in some circumstances, its individual employees could face prosecution for failure to handle personal data in accordance with the legislation.

2.0 Scope

This policy sets out how the council will manage the lawful and fair handling of personal data in line with the current data protection legislation and ensure that all personal data processed by or for the authority is subject to appropriate safeguards to ensure compliance with the relevant data protection legislation.

It applies to all personal and special categories of personal data held by or on behalf of the council and to all persons processing this data. This includes but is not limited to staff, elected members, contractors, consultants and third party processors (collectively referred to as data users).

3.0 Policy outcomes

Data Protection Policy outcomes	Links to corporate outcomes
• Accurate relevant personal information protected and maintained to ensure its confidentiality, integrity, relevance and availability to enable effective delivery of services. • Well informed staff and elected members who feel supported to ensure the accuracy and protection of the information they use.	• Effective management • Effective Partnership working • Knowledge of our customers and communities. • Councillors and staff with the right knowledge, skills and behaviours

4.0 Data Protection Policy

The council is committed to ensuring we meet the requirements of the current data protection legislation. The council fully endorses and adheres to the six Data Protection Principles which are set out in the GDPR and summarised below:-

Personal data must be:
a) processed lawfully, fairly and in a transparent manner

b) collected for specified, explicit and legitimate purposes
c) adequate, relevant and limited to what is necessary
d) accurate and where necessary kept up to date
e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed
f) processed in a manner that ensures appropriate security

The council is responsible for compliance with the principles and must be able to demonstrate this to data subjects and the Information Commissioners Office ICO.

The council will implement procedures which aim to ensure that all data users who have access to any personal data held by or on behalf of the council are fully aware of and abide by their duties under the General Data Protection Regulation, Data Protection Act and any other relevant legislation.

4.1 Notification

The council will maintain it's entry in the register of notifications held by the ICO, the registrations relating to the Electoral Returns Officer, and will manage the individual councillors registration on their behalf.

4.2 Information Asset Management/Records of Processing Activities

The council will maintain an information asset register/ record of processing activities which details the types of personal data held by the organisation, why it is held, how it is used, the lawful basis for it's use, who it is shared with, how long we will retain it and its disposal method.

4.3 Data Protection Officer (DPO)

As is required of all statutory bodies the council will appoint a Data Protection Officer.

The post holder will be responsible for ensuring the council works towards and maintains good standards of data protection and management in line with the current data protection legislation. They will also manage complaints and breach investigations, and gather and share information/make recommendations on how the council manages information security, data protection and other related subjects.

4.4 Training & Awareness

All staff (including contractors working with the organisation for a period of more than 3 calendar months) and councillors must undertake mandatory data protection training provided by the council's Data Protection Officer. Training will be provided at regular intervals throughout the year to ensure all new staff are able to attend and will be incorporated into member induction procedures.

Staff working with third party processors (i.e. contractors who manage/process personal data on our behalf) will liaise with the Data Protection Officer to ensure processor agreements are in place and that suitable training is provided to the staff at the processing organisation.

The Data Protection Officer will undertake to provide regular awareness raising campaigns and information to support staff in ensuring personal data is processed lawfully, fairly and in a transparent manner and in line with relevant data protection legislation.

4.5 Responsibilities of individual data users

All data users should familiarise themselves with the key elements of data protection including what constitutes personal data and special categories of personal data and understand how this relates to their area of work. All staff must take advice from the council's Data Protection Officer when required.

Heads of Service and Middle Managers must ensure data protection procedures are implemented in their service areas and that their teams are appropriately trained in Data Protection.

Team leaders must ensure all staff within their teams understand what constitutes personal data and are familiar with the correct procedures for secure storage and disposal of personal data, breach reporting, data protection impact assessments and information sharing in line with the guidance developed by the Data Protection Officer.

All staff must ensure when starting a new project, policy or way of working or reviewing a working procedure or policy that they consider whether a Data Protection Impact Assessment is required and liaise with the DPO accordingly.

All staff must also ensure they understand the data protection procedures and guidance provided in relation to the management of, security of, retention of and sharing of personal data and how this relates to their role.

4.6 Data Subjects Rights

The council will ensure that appropriate procedures and guidance are in place to support any individual data subject in exercising their rights over the data the council holds about them.

These rights include:

- the right to access the data (subject access request);
- the right to have inaccurate data rectified;
- the right to erasure (unless the data controller has a legal obligation/public task reason for processing the data);
- the right to restriction of processing;
- the right to data portability (this only applies to data where consent has been given as the legal basis for processing or where the data subject has entered into a contract with the council);
- the right to object to data processing; and
- the right to prevent significant decisions being made about them by solely automated means or to prevent profiling of their personal data.

The council will publish this advice as part of their privacy statement on the public website and will make this information available via any method of collection of personal data we undertake to ensure all relevant data subjects are aware of their rights and how to exercise them.

4.7 Information Sharing

The council will only disclose personal data to third parties when it is fair and lawful to do so in accordance with data protection legislation and with any Information Sharing Agreements.

The council undertakes to ensure appropriate security measures are in place to protect any personal data which it is required to or enabled to share with a third party.

Where sharing of information is established routinely as part of a process the council will ensure this is communicated as appropriate to our customers, staff and other data subjects via our privacy notices given at the point of collection of the data.

All routine data sharing will be appropriately documented as part of the information asset register/register of processing activities and will be monitored and reviewed by the Data Protection Officer.

4.8 Information Security and Information Security Breaches

The council will ensure that appropriate security measures are in place to protect the personal data/special categories of personal data given to us by our customers, staff, partners and elected members.

If a breach of security occurs the council and specifically the Data Protection Officer will ensure the breach management procedure is followed and, in line with guidance from the Information Commissioners Office (ICO), will self report any reportable breach within 72 hours of becoming aware of the breach.

4.9 Contracts and Service Level Agreements

The council will ensure all contracts and service level agreements where personal data is processed make reference to data protection legislation as appropriate.

The council will also undertake to carry out checks to satisfy themselves that the contractors are upholding the elements of their contract which refer to data protection.

4.10 Special Category/Sensitive Personal Data

Special Category data (sensitive personal data) is personal data revealing the following types of information about a data subject:

- race;
- ethnic origin;
- politics;
- religion;
- trade union membership;
- genetics;
- biometrics (where used for ID purposes);
- health;
- sex life; or
- sexual orientation.

This type of personal data is deemed more sensitive and therefore requires additional safeguards to be put in place to protect it and for the council to be explicitly clear as to why it is processing it.

The council will ensure all personal data is processed in line with the relevant data protection legislation. All sensitive/special category personal data will only be processed if the conditions of the Data Protection Act 2018/General Data Protection Regulation are met or where an exemption from the above legislation applies.

The council does not routinely hold data relating to criminal convictions but will apply the conditions of the Data Protection Act 2018 and the Law Enforcement Directive.

4.11 Accuracy of personal data

The council will ensure procedures are in place to check and maintain the accuracy of the personal data that we process.

The council will also ensure data shared with other agencies/partners or third party processors is accurate at the point of sharing and kept updated where appropriate.

4.12 Retention of personal data

The council will not hold personal data for longer than is required either by law or for the purposes of service delivery whichever is longer. A detailed schedule of retention periods will be maintained by the Data Protection Officer and service managers and where electronic systems allow, automated retention policies will be enforced.

Where no system is available or where data is held in manual files retention exercises will be carried out at appropriate regular intervals to ensure the council does not hold personal data it no longer requires.

4.13 Privacy by design

The council will ensure procedures are in place to ensure a privacy by design approach is taken to any new projects, policies or procedures which involve/relate to the processing of personal data. In doing so this will ensure privacy and data protection are built into any new systems/processes and policies from the start and are monitored throughout the development, implementation and beyond.

The Data Protection Officer will offer support and guidance in the completion of Data Protection Impact Assessments (DPIA) and will monitor any action plans put in place for data protection issues in conjunction with the appropriate staff.

4.14 Audit & Review

The council will audit compliance with this policy or a regular basis and ensure that any incidents involving breaches of the policy or the relevant data protection legislation are recorded, analysed and acted upon.

The council will ensure this policy is reviewed at regular intervals (no more than 3 years) to ensure relevance and to monitor compliance with relevant legislation.

5.0 Next steps

The council already has a data protection action plan in place which will continue delivery of data protection measures in line with the requirements of the relevant data protection legislation.

6.0 Glossary of terms

Term	Definition
General Data Protection Regulation (GDPR)	EU data protection legislation which came into force on 25/05/2018
Data Protection Act 2018 (DPA 2018)	UK enactment of GDPR including areas where member states could determine additional measures. Came into force 23/05/2018
Data users	Any individual or organisation who processes personal data on behalf of, for or in conjunction with the council.
Data subject	Any individual who data is held about
Data Protection Impact Assessment (DPIA)	Assessment of impact of any proposed work (new project, system, policy/procedure or review of any current working arrangements including all of the above) where personal data is involved. This is a requirement of the new data protection legislation GDPR / DPA2018.
Third Party Processor/ Processor Agreements	An organisation the council contract to provide services on its behalf who process customer or staff/elected members personal data on behalf of the council. Any third party processor will need to have a clear agreement in place with the council which will detail their responsibilities and ours in relation to Data Protection Legislation (this may be built into the overall contract documents).
Information Commissioners Office (ICO)	The regulator for all data protection and freedom of information legislation in the UK.
Personal Data Breach (data security breach)	A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

Appendices:

Appendix A – Equalities impact assessment – initial assessment
Appendix B – Data Protection Impact Assessment – initial assessment

APPENDIX 2

Privacy Impact Assessments

Privacy by design is an approach to projects and review of existing working practices that promotes privacy and data protection from the start.

This approach is a requirement of the General Data Protection Regulations and Data Protection Act 2018, and it will help East Northamptonshire Council ensure that privacy and data protection is a key consideration in the early stages of any project and then throughout its lifecycle. For example when:

- building new IT systems for storing or accessing personal data;
- developing legislation, policy or strategies that have privacy implications;
- starting a new data sharing initiative; or
- using personal data we already hold for new purposes.

Taking a privacy by design approach helps us to minimise privacy risks. Designing projects, processes, products or systems with privacy in mind can lead to benefits which include:

- Identifying potential problems at an early stage, which means they should be simpler and less costly to fix.
- Increased awareness of privacy and data protection across our organisation.
- Help us to reduce the likelihood of breaches.

Privacy impact assessments (PIAs) are a tool used by East Northamptonshire Council to identify and reduce the privacy risks of your projects. A PIA 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 information.

Projects which might require a PIA

A PIA should be applied to any project which involves the use of personal data or to an activity which could have an impact on the privacy of an individual such as:

- A new IT system for storing and accessing personal data.
- A data sharing initiative where two or more organisations seek to pool or link sets of personal data.
- A proposal to identify people in a particular group or demographic and initiate a course of action.
- Using existing data for a new and unexpected or more intrusive purpose.
- A new surveillance system, especially one which monitors members of the public.
- A new database which consolidates information held by separate parts of the council.
- Legislation, policy or strategies which will impact on privacy through the collection of use of information or through other monitoring.

How does the process work?

Please complete the initial assessment form below and return to Kirsty Squires (Data Protection Officer) by email to ksquires@east-northamptonshire.gov.uk

If you are unsure about any element of the form please contact Kirsty for advice.

If you answer yes to any of the questions on this initial assessment please complete the full form. Kirsty is available to support you with this if required.

Privacy Impact Initial Assessment Form

For ease, where the term 'project' is used, it will refer equally to a project, review of a process, or a policy for the purposes of the assessment.

Policy/Project Name:	Data Protection Policy
Reference/Identifier (e.g. Project number)	n/a
Name of project/policy owner:	Kirsty Squires
Date of assessment:	30 August 2018

Will the project/policy result in the collection/use/control of <u>any</u> Personal Data?

	Please tick	Next step…
No		If no, you need take no further steps. Save and submit this form with your policy, or save it with your project documentation.
Yes	X	If yes, answer the questions below. Submit the completed form to the Information Governance Manager.

For projects/policies utilising personal data, please answer all questions. Please provide relevant explanations/descriptions:

Will the project involve the collection of new information about individuals?	No
Will the project compel individuals to provide information about themselves?	No
Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?	No. The policy and supporting procedures will give clear guidance on how to ensure we only collect data required.
Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?	No
Does the project involve you using new technology which might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition.	No

Will the project result in you making decisions or taking action against individuals in ways which can have a significant impact on them?	No. The policy will provide guidance to ensure privacy impact assessments are carried out to investigate how council projects will impact on data collected and decisions made.
Is the project likely to raise privacy concerns or expectations? For example, using health records, criminal records or other information that people would consider to be particularly private.	No
Will the project require you to contact individuals in ways which they may find intrusive?	No

Initial Equalities Impact Assessment

APPENDIX 3

Title of proposal being assessed:	*Data Protection Policy*
What type of proposal is this an assessment of?	*Policy - New*
What are the aims and/or objectives of the proposal and the intended outcomes?	*To ensure compliance with relevant data protection legislation*
Who is intended to benefit from this proposal?	*All staff, elected members and customers*
Who are the main stakeholders in relation to the proposal?	*Staff, elected members and customers*
How is the success of the proposal to be measured?	*via the GDPR implementation plan and regular audit of compliance*
Name of person completing Initial Screening:	*Kirsty Squires*
Job title / role of person completing Initial Screening:	*Data Protection Officer*
Date of Initial Assessment	*30/08/2018*

Instructions: For **every** category in column A, below, submit a positive, negative or neutral assessment by entering an **x** in the relevant cell. Add an explanation in the Reason box, where applicable, including a specification of any sub-group affected. There may be both a positive and negative impact for the same category (e.g. a policy may be positive for young children but negative for older people).

Equality Group	Positive Impact	Negative Impact	Neutral Impact	Explanation and Evidence (e.g. description of elements of the proposal, data held, consultation results, customer feedback)
Gender:				
Consider Women/Girls, Men/Boys, Transgender individuals.			x	
Sexual Orientation:				
Consider, for instance: Lesbians, gay men and bisexuals Any other sexual orientation			x	
Race/Ethnicity:				
Consider, for instance: • White British people, • White non-British people • Asian or Asian British people • Black or Black British people • Chinese people • People of mixed heritage • Travellers (Gypsy/Roma/Irish heritage) • People from any other ethnic groups • People who do not have English as their first language			x	
Disability:				
Physical impairment, e.g mobility issues which mean using a wheelchair or crutches.			x	
Sensory impairment, e.g blind/having a serious visual impairment, deaf/having a serious hearing impairment.			x	
Mental health condition, e.g depression or schizophrenia			x	
Learning disability/difficulty, e.g. Down's syndrome or dyslexia, or cognitive impairment such as autistic spectrum disorder			x	
Long-standing illness or health condition, e.g. cancer, HIV. Diabetes, chronic heart disease or epilepsy			x	
Other health problems or impairments *(please specify if appropriate)*			x	
Marriage and Civil Partnership:				
People in a Marriage or Civil Partnership			x	
Pregnancy and Maternity:				
People who have just had a baby or who are pregnant.			x	
Age:				
Older People (60+)			x	
Children and Young People (see guidance for definition)			x	
Religion/Belief:				

Consider, for instance: • Christian • Hindu • Muslim • Sikh • Buddhist • any other religion or belief (including holding no belief)			x	
Other Potentially Affected Groups				
Rural Isolation - People who live in rural areas e.g isolated geographically, lack of internet access			x	
Socio–economic Exclusion – e.g. people who are on benefits, have low educational attainment, single parents, people living in poor quality housing, people who have poor access to services, the unemployed or any combination of these and the other protected strands			x	
Any other potentially affected groups *(please specify)*				n/a