NORTH OF TYNE COMBINED AUTHORITY

DATA PROTECTION AND CONFIDENTIALITY POLICY

If you have any questions relating to this document, data protection in general or you want report a data protection incident, please contact the Information Governance Team via dataprotection@newcastle.gov.uk or call 2116500 (26500)

1. Scope

This policy applies to all employees, contractors, agents, consultants, or other partners of the Combined Authority who process personal information held by, or on behalf of the North of Tyne Combined Authority (the Combined Authority).

This policy covers all personal data; however, they are held, on paper or in electronic format. It also covers the rights of individuals (data subjects) who wish to see information the Combined Authority holds about them (by submitting a Subject Access Request).

2. Purpose

The purpose of this policy is:

- To ensure compliance with Data Protection Legislation:
    - the General Data Protection Regulation (GDPR) 2018
    - The Data Protection Act 2018

This will be achieved by ensuring that personal information is processed as set out in this policy and as required by the GDPR.

- To ensure that all information and information systems upon which the Combined Authority depends are adequately protected to the appropriate level. This includes IT infrastructure for the retrieval, sharing and dissemination of business-critical data and conducting daily transactions.
- To ensure that all staff and other users are aware of their responsibility for the security of Combined Authority information.
- To ensure that all staff and other users are aware of their responsibilities for processing personal information under the Data Protection Act 2018.
- To ensure that all staff and other users are aware of their accountability
- To ensure that information is handled securely.
- Information asset owners are identified for all major information assets and that there is clear responsibility for maintaining appropriate controls.

This policy does not intend to replace the Data Protection Legislation, it merely aims to simplify the content. It may be necessary to refer to the relevant Data Protection legislation, in order to ensure compliance with requirements. Advice on the complying with this policy can be sought from the Information Governance Team (Contact details are available at the end of this policy)

3. Introduction

3.1 The Combined Authority is fully committed to compliance with the requirements of Data Protection Legislation. It is a legal requirement that the Combined Authority complies with the regulation, and all elected members, employees, contractors, agents, consultants and partners of the Combined Authority have a statutory responsibility to ensure compliance.

3.2 The Combined Authority will therefore follow procedures which aim to ensure that everyone who manages and handles personal information for, or on behalf of the Combined Authority, is fully aware of, and abide by their duties and responsibilities under the Data Protection Legislation.

3.3 In order to operate efficiently, the Combined Authority must when necessary, process (collect and use) personal information about people with whom it works and conducts its business. These people may include members of the public, current, past and prospective employees, clients, customers and suppliers. In addition, the Combined Authority may be required by law to collect and use personal information in order to comply with the requirements of central government. Personal information must be handled and dealt with properly and securely, however it is collected, recorded, used, deleted and disposed of. There are safeguards within the GDPR to ensure this.

3.4 The Combined Authority regards the lawful and correct treatment of personal information as very important to its successful operations, and to maintaining confidence between the Combined Authority and those with whom it carries out its business. The Combined Authority will ensure that it treats personal information lawfully and correctly.

4. Definitions

Descriptions of the data protection terms used in this policy can be found in the glossary at the end of this policy document.

4.1 Personal data is information which relates to a living individual who can be identified:

- from that data, or
- from that data when combined with other information which is either in the Combined Authority's possession or likely to come into the Combined Authority's possession.

4.2 For the purposes of Data Protection legislation, and the Combined Authority's Data Protection and Confidentiality Policy, it is safest to assume that all information about a living, identifiable individual is personal data and should be dealt with accordingly.

4.3 Special category data can include information relating to:

- Religious or philosophical belief
- Sexual life or sexual orientation
- health data
- trade union membership
- Political opinions
- Commission or alleged commission of an offence
- Proceedings for any offence committed or alleged to have been committed
- Biometric and genetic data

4.4 Special category data must only be used for approved purposes e.g. equal opportunities monitoring and access to this data must be restricted to those who have a need to know. They should never be kept in a generally accessible record or file. Advice on the issue of sensitive data can be sought from the Information Governance team.

5. The principles of the General Data Protection Regulation (GDPR) 2018

5.1 The seven principles which form the basis of the Regulation provide the foundation for the appropriate control and processing of personal data. They are as follows:

5.1.1 Principle 1 - Legality, transparency and fairness

Data must be processed fairly and lawfully. Nobody should be deceived or misled about the purpose for which their data is to be processed.

5.1.2 Principle 2 - Purpose limitation

Personal data should be collected for specified, legitimate and explicit purposes and must not be further processed in a way which is incompatible with such purposes.

5.1.3 Principle 3 - Minimisation

The data must be relevant, adequate, and limited to what is necessary in relation to the purposes for which that data is processed.

5.1.4 Principle 4 - Accuracy

The personal data must be accurate when recorded, and accuracy must be maintained throughout the lifecycle of the data. Every reasonable step must be taken to update inaccurate personal records.

5.1.5 Principle 5 - Storage limitation

Personal data must not be kept for any longer than is necessary for the purpose for which it was obtained.

5.1.6 Principle 6 - Integrity and confidentiality

Personal Data shall be processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using technical or organisational measures.

5.1.7 Principle 7 - Accountability

Both data controllers and data processors have responsibility for and must be able to prove and demonstrate compliance with all principles outlined within the GDPR.

6. Processing personal data

6.1 The definition of processing in relation to data protection is very wide. Obtaining, holding, filing, organising, transmitting, retrieving, disseminating, disclosing and destroying of data are all deemed to be processing in addition to any other process that is carried out on the data.

6.2 There is a requirement to inform the general public why the Combined Authority needs information about them, how this is used and to whom it may be disclosed.

6.2.1. The Combined Authority will ensure that individuals are made aware of personal information being held by the Combined Authority and how this information is being used, held, who can access it, with whom it is being shared and for how long it will be kept. This will be by Privacy Notices and will happen where the use of personal information is not obvious.

6.2.2 There is a corporate Privacy Notice on the Combined Authority's website. Additional more detailed, service or functional based Privacy Notices will (where applicable) be clearly stated on written literature, on Combined Authority web pages and verbally, if individuals are being spoken to face to face or by telephone.

6.2.3 There are instances, as permitted by Data Protection legislation when individuals will not be made aware that their information is being processed, such as when the processing is in connection with the prevention and detection of crime.

6.3 Employees, and others acting on behalf of the Combined Authority must only have access to personal data that is necessary in order to carry out their duties and responsibilities.

6.4 All forms used to obtain personal data, such as application forms or registration forms must include a Privacy Statement in clear and plain language, providing the following:

6.4.1 Stating the purpose/s for which the information is required, who it will be shared with, how long it will be retained and how it will be destroyed. It should also include a link to a more detailed Privacy Notice. The Information Governance team can support teams to write clear Privacy Statements and Privacy Notices.

All personal data obtained, must always:

6.4.2 Be reviewed regularly to check that all of the information asked for is still required and necessary. To ensure we comply with the minimisation principle.

6.4.3 Be checked for the accuracy of all data before it is used for any processing. If in doubt about the accuracy of the data, it must be referred back to the data subject for confirmation. To ensure we comply with the accuracy principle.

6.5 Personal data must be collected and handled in a way that complies with the Regulation and meets the seven principles above. This imposes a duty on the Combined Authority to ensure that individuals are made aware of the uses that will be made of the information that they supply and give their consent to this.

6.6 If an outside agency provides data to the Combined Authority, the Combined Authority has the right to ask the agency to confirm in writing that the data was obtained fairly and lawfully, in compliance with the Regulation.

6.7 Where personal data is provided for the purpose of placing a contract to which the data subject is a party then such data is considered to be fairly and lawfully obtained.

7 Handling of personal and special category information

7.1 The Combined Authority will through appropriate management and the use of strict criteria and controls.

7.1.1 Ensure everyone managing and handling personal information understands that they are contractually responsible for following good data protection practice

7.1.2 Ensure everyone managing and handling personal information are adequately trained and supervised to do so

7.1.3 Observe fully conditions regarding the fair collection and use of personal information

7.1.4 Meet its legal obligations to specify the purpose for which information is used

7.1.5 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

7.1.6 Ensure the quality of information used

7.1.7 Apply strict checks to determine the length of time information is held

7.1.8 Take appropriate technical and organisational security measures to safeguard personal information

7.1.9 Ensure that personal information is not transferred abroad without suitable safeguards

7.1.10 Ensure methods of handling personal information are regularly assessed and evaluated

7.1.11 Ensure that the rights of people about whom the information is held can be exercised fully under the Data Protection legislation. Please see Section 14.

8 Responsibilities

8.1 The Data Protection Officer will monitor the Combined Authority's compliance with the Data Protection legislation, ensure that the Data Protection Policy is implemented, advise and consult on responses to data Subject Access Requests and make regular reviews of this policy and associated documentation.

8.2 Whilst the Combined Authority's Director of Policy & PerformanceService is ultimately responsible, both personal and corporate responsibility applies. The North of Tyne Combined Authority is registered as a Data Controller and therefore has a corporate responsibility for compliance with all Data Protection legislation however there is also a personal responsibility on all employees for ensuring compliance with the principles of the Regulation by complying with this policy.

8.3 Information Asset Owners and Line Managers must ensure that those staff processing personal information are appropriately trained and with regard to the requirements of this policy and with Data Protection legislation.

8.4 The Information Asset Owners in Combined Authority service areas are responsible for ensuring that they and staff in their service are aware of the relevant documentation. Lead Officers will progress relevant data protection Subject Access Requests (See paragraph 13 below) and liaise with the Combined Authority's Information Governance team on any issues which may arise.

9 Data Breaches

9.1 All data protection breaches must be reported to the Information Governance team immediately at the point that the incident becomes apparent. The Information

Governance team have 72 hours from being notified of a breach to report to the Information Commissioner's Office (where feasible). It is the responsibility of the service to carry out an investigation into an incident with support and guidance provided from the Information Governance Team. All Data Protection incidents are logged centrally by the Information Governance Team.

10 Data Protection Impact Assessments (DPIA)

10.1 Data Protection Impact Assessments (DPIAs) are carried out on all Combined Authority significant decisions and as part of the start of any project, if personal information is involved and there are risks to the privacy of individuals. The DPIA will consider the risks of complying with legislation such as the GDPR and document work required to resolve any design issues, including the alternatives considered and why the option chosen was selected.

10.2 The size of the DPIA should reflect the scale of the project or change and the following questions should be considered when deciding whether or not to carry out a DPIA:

1. Will the project/decision involve the collection of new information about individuals?
2. Will the project/decision require individuals to provide information about themselves?
3. Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?
4. Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?
5. Does the project/decision involve you using new technology that might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition software.
6. Will the project/decision result in you making decisions, or taking action against individuals in ways that can have a significant impact on them? (including automated decisions).
7. Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records or other information that people would consider to be private.
8. Will the project/decision require you to contact individuals in ways that they may find intrusive?

11 Relevant and adequate data

11.1 The Combined Authority must process only that information which is necessary to fulfill the business requirement, or which is needed to comply with legal

requirements. For example, it is not necessary to ask for someone's date of birth if all you need to know is that they are over 18.

12 Collecting and maintaining accurate data

12.1 It is important therefore that all appropriate measures are put in place to verify the accuracy of data when it is collected, especially when any significant decisions or processes depend upon the data. Errors in personal data that could or does cause data subjects damage or distress could lead to the Combined Authority being prosecuted.

12.2 There is a requirement to ensure that data is kept up to date throughout the lifecycle of the data.

12.3 Users of software will be responsible for the quality (i.e. accuracy, timeliness, and completeness) of their data by carrying out their own quality assurance and participating as required in quality assurance processes.

13 Keeping data only as long as necessary

13.1 Retention periods should be defined for personal data and procedures put in place to ensure compliance.

13.2 Retention periods must be for clear business purposes/and or legal basis, and this must be documented to identify why certain records are retained for certain periods of time. Please refer to the Combined Authority's retention schedule.

13.3 When no longer required, data must be deleted or disposed of securely.

14 Rights of individuals

14.1 Safeguarding the rights of data subjects

14.1.1 The GDPR provides the following rights for individuals:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling.

14.2 Subject Access Requests (SARs).

14.2.1 The Combined Authority must make available details of how individuals can request access to their data. This is known as a Subject Access Request (SAR).

14.2.2 Requests for personal information:

- Must explain the information required (we may seek further clarification if this is too broad to enable a successful search).
- Must be accompanied by identification to help prevent fraudulent requests.
- Can be made via a 3rd party, such as a solicitor or someone holding power of attorney, with the permission of the data subject.

14.2.3 The Combined Authority may be entitled to refuse any requests on procedural grounds such as when the above points are not complied with.

14.2.4 If we are able to release the information, we will collate it, advise of the source and generally provide a permanent copy. We aim to provide it within 1 month as required by the regulation. For complex and numerous requests, a 2 month extension can be used.

14.2.5 If we decide to deal with a request for information under another information request regime or as a combination of regimes we will advise accordingly. An example is when a request for the non-personal information is made under the Regulation. In this instance the request would be considered under the Freedom of Information Act.

14.2.6 If the information cannot be released within the timeframe there must be a valid reason for the delay, we will advise the requester and they will be kept informed of progress and given access to information as it becomes available. The information provided will be in permanent form, such as a written document, unless we are unable to provide a permanent copy.

14.2.7 If we are unable to provide some or all of the information because, for example it is exempt from disclosure, we will explain this in writing to the requester.

14.2.8 We will provide advice with each request about how to make a complaint, and how to appeal to the ICO.

14.3 Requests for inaccurate information to be rectified, erased, destroyed or blocked

13.3.1 Individuals can ask that inaccurate personal information is corrected or deleted.

14.4 Prevent processing likely to cause damage or distress

14.4.1 Individuals can ask the Combined Authority to stop handling their personal information if it is causing or is likely to cause substantial damage or distress to that individual or another person.

14.5 Prevent processing for direct marketing

14.5.1 Individuals can ask that their personal information is not used or is no longer used for direct marketing.

14.6 Prevent automated decision taking

14.6.1 Individuals have the right to prevent decisions, which significantly affect them; being made just by automated means.

15 Requests for disclosure of personal information by third parties

15.1 The GDPR has an exemption that allows third parties to request personal information in some circumstances.

15.2 Personal information may be disclosed to a third party under the GDPR if the request is in connection with, for example for the prevention or detection of crime

15.3 For other requests by third parties, we will only provide information to third parties if there is a legal requirement to do so or as part of a data sharing agreement in line with our corporate Privacy Notice.

16 Keeping data secure

16.1 The Combined Authority acts as custodian of personal data and must therefore ensure that necessary and sufficient precautions are in place to prevent misuse or unauthorised access to data as well as having security measures in place to prevent loss or damage to data.

16.2 Where outside bodies process or hold any of the Combined Authority's personal data then the Combined Authority must be satisfied that the data is held securely and with due regard to the obligations of the GDPR.

17 Transfer of data

17.1 Data must not be transmitted or transferred out of the European Economic Area (i.e. the EU member states) unless the country they are being transferred to has the same or equivalent standards of Data Protection. Prior to any transfer of personal

data, a legal agreement must be put in place and approved by the Information Commissioner's Office (Supervisory Authority, UK). This has implications for data placed on the Internet and use of email where servers are based abroad.

17.2 If information is required to be transferred abroad then advice on this process should be sought from the Information Governance team in the first instance.

18 Training and awareness

18.1 All staff will need to be aware of the Combined Authority's Data Protection Policy. To help staff understand the basic principles, data protection statutory training will be provided on an annual basis.

18.2 Some members of staff will require further training and guidance. Those members of staff will be identified through their work with initial discussion with their line manager. The Information Governance Team can advise on appropriate training where this need is identified.

18.3 When staff join the Combined Authority, it is important that they are introduced to their basic responsibilities under the GDPR. To ensure that they are aware, they will need to complete the mandatory learning modules on the GDPR.

19 Compliance

19.1 Any violation of this policy will be investigated and if the cause if found to be willful disregard or negligence, may be treated as a disciplinary offence. All disciplinary proceedings are coordinated through the HR Department.

20 Implementation

20.1 This policy is effective immediately.

21 Monitoring and review

21.1 This policy will be monitored by the Information Governance Board and will be reviewed every two years or where there are changes to Data Protection legislation.

22 Useful contacts

Information Governance Team

6th Floor Civic Centre

Newcastle upon Tyne

NE1 8QH

Email: dataprotection@newcastle.gov.uk

Phone: 0191 2116500

The Information Commissioner's Office via www.ico.org.uk

23 Glossary

Biometric data: personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data.

Consent: any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

Data controller: is the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by the Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

Data processor: a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

Data subject: a natural person whose personal data is processed by a data controller or processor.

Genetic data: personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question.

Personal data: any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Personal data breach: a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Privacy impact assessment: or Data Privacy Impact Assessment. A process designed to help organisations identify and mitigate privacy risks associated with proposed data processing activities. For further information, please contact the Information Governance team.

Principles: the fundamental principles embedded within the GDPR which set out the main responsibilities for organisations.

Processing: any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Profiling: any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

Pseudonymisation: the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, as long as such additional information is kept separately and technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

Restriction on processing: the marking of stored personal data with the aim of limiting their processing in the future.

Right of access: entitles the data subjects to have access to information about the personal data being processed by the data controller.

Special categories of personal data: personal data revealing a data subjects racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership or the processing of genetic data, biometric data for the purposes of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.