DATA PROTECTION POLICY

The General Data Protection Regulation (GDPR) and the DATA PROTECTION ACT 2018

Version 2 - 11 April 2019

Produced by - SG Renwick
Steve.renwick@togetherforchildren.org.uk

Contents

1. Introduction

This Data Protection Policy sets out Together for Children's (TfC) approach to handling personal information in accordance with the Data Protection Act (DPA) 2018 and the General Data Protection Regulation (GDPR) and provides a framework for understanding the requirements of the legislation.

The DPA and GDPR seek to balance the rights of individuals and the use of personal data, including fact and opinion about individuals, where there is a legitimate basis for that use. They set out standards and rules and place obligations on those who process information while giving rights to those who are the subject of the data (data subjects). These standards and rules cover the collection and use of information, the quality and security of the information and the rights of individuals regarding information about themselves.

The policy provides an overview of the main obligations for Officers and Board Members in dealing with personal information so they can comply with the transparency, accountability, data processing, and other principles established under this legislation and the exercise of the individual rights.

2. Registration

2.1 TfC is registered with the Information Commissioner (ICO) as a Data Controller for the processing of living individuals' personal information.

3. Statement of policy

3.1 TfC collects and uses information about people it works with to operate and carry out its functions. In a number of circumstances, TfC is required by law to collect and use information.

TfC is committed through its policy, procedures and guidelines to ensure that it will:

- comply with both the law and good practice
- respect individuals' rights
- be open and honest with individuals whose data is held
- provide training and support for staff who handle personal data, so that they can act confidently and consistently

3.2 At the heart of the Act is the need to protect personal information (otherwise known as personal data) and put additional protection in place for the special categories of sensitive personal data.

3.3 This means that when TfC collects and uses personal information, it must handle it and deal with it according to the principles of Transparency and Accountability and the Data Processing Principles.

4. Transparency and Accountability

4.1 TfC will maintain information for data subjects about its data collection and data handling arrangements, advising what the collected data is being used for, how long it is kept and who it will be shared with. TfC will make this available to data subjects through the publication of Privacy notices.

4.2 TfC will maintain a series of retention schedules setting out in general terms the period of time data in a specified category will be retained. These retention schedules, echo those of the Council as updated from time to time, and will be made available on the council website www.sunderland.gov.uk .

4.3 TfC will maintain records of data processing, detailing its data processing activities and the measures it has adopted to achieve compliance with the Data Processing Principles.

4.4 TfC will arrange for a Data Protection Impact Assessment (DPIA) (also known as Privacy Impact Assessment (PIA)) to be carried out when proposals under consideration are likely to result in a high risk to the rights and freedoms of natural persons and seek the advice of the Data Protection Officer in carrying out such assessments.

4.5 TfC will consult the Information Commissioner prior to processing where DPIA indicates that the processing would result in a high risk to the rights and freedoms of natural persons in the absence of measures taken by TfC to mitigate the risk.

5. The Data Processing Principles

5.1 TfC, as data controller, is responsible for, and must be able to demonstrate compliance with the six principles relating to processing of personal data (accountability).
TfC, working through its staff and agents, must follows the data processing principles to comply with the Act. The principles set the framework of legitimate reasons for an organisation to process or use personal information.

5.2 The Principles are legally enforceable and failure to process personal information in accordance with them, means individuals and TfC can be considered in breach of the Data Protection Act.

5.3 The six principles, which form the basis of the Act, state that data must be:

1. **Processed lawfully, fairly and in a transparent manner in relation to the data subject (lawfulness fairness and transparency)**
   The data subject must be informed about the purpose for which their data is to be processed, unless exceptions apply.

2. **Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes**
   Personal data can only be obtained for specified and lawful purposes, or with permission from the data subject for each purpose.

3. **Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (data minimisation)**
   The data must be sufficient to meet their purpose but not provide more information than the purpose requires or provide information outside the scope of the purpose.

4. **Accurate and, where necessary, kept up to date (accuracy)**
   Every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased of rectified without delay.

5. **Kept in a form which permits identification of data subjects for no longer than is necessary**
   Personal data must not be kept for any longer than is necessary for the purpose for which it was obtained. Pseudonymisation and anonymisation should be considered if information is to be kept for archiving, research or statistical purposes.

6. **Processed in a manner that ensures appropriate security of the personal data (integrity and confidentiality)**
   This includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures

6. Scope

6.1 The policy applies to all processing of personal data by and on behalf of TfC. The policy covers all data that falls within the definition of personal data under the Act.

6.2 **Personal data** means any information relating to an identified or identifiable natural person.

An **identifiable natural person** is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, number, location data or online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

6.3 The policy applies equally to full time and part time employees on a substantive or fixed term contract and to associated individuals who work for TfC including agency staff, contractors and others employed under a contract of service.

6.4 The policy also applies to Board Members in their role as a Member of the TfC Company Board of Directors.

6.5 The policy covers all personal information that TfC holds in either electronic or paper format or file system.

6.6 The policy applies throughout the life cycle of the personal data from the time it is created or arrives within TfC to the time it is either destroyed or preserved permanently.

7. How We Use Personal Data

7.1 Legal basis for processing

We process personal information where there is a relevant legal basis to do so in data protection law.

These legal grounds include where;

- the data subject has given consent to the processing for the specific purposes
- processing is necessary to perform or take preparatory steps for a contract with the data subject
- processing is necessary to comply with one of TfC's legal obligations
- processing is necessary to protect the vital interests of the data subject or another person
- processing is necessary to carry out a task in the public interest or the exercise of TfC's official authority
- processing is necessary for the purposes of legitimate interests a third party or TfC is pursuing, where those purposes do not form part of TfC's public task

7.2 Sensitive personal data

7.2.1 All staff must recognise how to identify sensitive personal information and how to process it lawfully and according to TfC policy. Staff should seek advice from the Data Protection Office if uncertain about how the following rules apply.

7.2.2 Sensitive personal data, known as a special category, is personal data consisting of information relating to:

- Racial or ethnic origin
- Political opinions, Religious beliefs or philosophical beliefs
- Membership of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992)
- Physical or mental health or condition
- Sexual life or sexual orientation
- Genetic or biometric data for the purpose of uniquely identifying a natural person
- Commission or alleged commission of any offence
- Any proceedings for any offence committed or alleged to have been committed, the disposal of such proceedings or the sentence of any court in such proceedings.

7.2.3 Special Category data (known as sensitive personal information) is given specific protection under GDPR. Information in these categories is particularly sensitive as processing could create significant risk to the rights and freedoms of an individual.

7.2.4 Sensitive personal data can only be processed where specified conditions are met.

- The data subject has given explicit consent to the processing for the specified purpose.
- Processing is necessary to carry out employment, social security and social protection law obligations, or exercise specific rights, authorised under the DPA.

- Processing is necessary to protect the vital interests of the data subject (life and death situations) where the data subject is physically or legally incapable of giving consent.
- Processing carried out by an organisation with a political, philosophical, religious or trade-union aim under conditions specified in the GDPR
- Processing relates to personal data the data subject has made public.
- Processing is necessary to establish, exercise or defend legal claims or when a court is acting in its judicial capacity.
- Processing is necessary for reasons of substantial public interest, on the basis of law, and proportionate to the aim pursued, respectful of the right to data protection and provides suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.
- Processing is necessary, and processed by or under the responsibility of a professional subject to the obligation of professional confidentiality for;
    - preventative or occupational medicine,
    - assessment of the employee's working capacity,
    - medical diagnosis,
    - provision of health or social care or treatment
    - the management of health or social care systems and services, or
    - under a contract with a health professional
- Processing is necessary in the public interest in the area of public health (principles of proportionality and professional confidentiality apply)
- Processing is necessary for archiving purposes in the public interest, or for scientific or historical research purposes

8. Individual Rights

8.1 TfC must observe and respect the data protection rights of individuals

8.2 The data protection principles support TfC in managing data in line with the individual rights. When managing data, TfC must ensure that any restriction of rights is proportionate to the purpose for which the information is shared. In assessing proportionality, it is also necessary to consider the impact on the data subject against the wider benefits of sharing the information.

8.3 Individuals, also known as data subjects, have the following rights;

1. **The right of Access by the data subject**
   The data subject has the right to obtain from the controller confirmation as to whether or not personal data concerning him/her are being processed and, where that is the case, to access their personal data and be given specified information about the processing

2. **The right to rectification**
   The data subject has the right to have personal data concerning him/her rectified without undue delay. This may include the right to have incomplete personal data completed, including by means of providing a supplementary statement.

3. **The right to erasure ('right to be forgotten')**
   The data subject has the 'right to be forgotten' where the retention of the data infringes DPA or GDPR requirements.

4. **The right to restriction of processing**
   The data subject has the right to obtain restriction of processing to preserve personal data in specified circumstances.

5. **The right to data portability**
   The data subject has the right to receive the personal data concerning him/her which he/she has provided to the controller in a structured, commonly used and machine-readable format and to transmit those data to another controller.

6. **The right to object**
   The data subject has the right to object to processing of personal data where the legal basis for processing is public interest task, or legitimate interests. The controller shall no longer process the personal data unless compelling legitimate grounds for the processing are demonstrated, which override the interests, rights and freedoms of the data subject, or for the establishment, exercise or defence of legal claims. The data subject has the right to object to processing for direct marketing purposes at any time.

9. Roles and Responsibilities

9.1 Board Members

This policy applies when Board Members handle personal information in their role as elected members, they do so on behalf of TfC.

9.2 Staff

This policy applies to all staff including contractors, consultants and volunteers employed to undertake TfC business. All staff are responsible for processing personal data lawfully and in accordance with TfC requirements. Failure to do so is a disciplinary matter and may be addressed formally or informally through TfC's performance management and disciplinary arrangements. Where appropriate, such failures will also be reported to professional bodies and police to consider further action.

All staff members have an obligation to report data protection breaches or contact the DPO if they have concerns of such a breach. This will provide them with access to advice on immediate steps to be taken to mitigate harm to data subjects and initiate an investigation into the circumstances and action to be taken to guard against future breaches. TfC's arrangements for reporting breaches are at Appendix C.

9.3 Board of Directors

The Board has overall responsibility for this policy and for ensuring that TfC, as a data controller under the Data Protection Act, and its staff complies with its legal obligations regarding the handling of personal information. In discharging this duty, the Board will maintain corporate arrangements for data protection within TfC as set out in this policy to protect personal information. By demonstrating TfC's commitment to the data protection principles of accountability and transparency and promoting good governance, all members of the Board have the lead role in developing a data protection culture within TfC.

9.4 Information Asset Owners

Directors, as Information Asset Owners, have responsibility for seeing that their service complies with the principles of the data protection act when processing personal data. Their responsibility includes ensuring that their staff are aware of their responsibilities under the Data Protection Act and are trained to discharge those responsibilities. The Director's role is to ensure that good Data Protection practice is established and followed and to:

- Ensure employees, including contractors, consultants and volunteers employed to undertake TfC business follow the data protection policy and procedures.
- Ensure appropriate resources are in place to enable compliance with the data protection policy.
- Ensure Data Protection Impact Assessments are carried out in relation to emerging proposals, as appropriate.

9.5 The Data Protection Officer and the Data Protection Office

The Council has appointed a Data Protection Officer to carry out the duties specified in the data protection legislation and this service is accessed by TfC under a Service Level Agreement.

The Data Protection Office is responsible for:

- Briefing senior managers on Data Protection responsibilities
- Reviewing and making recommendations for Data Protection and related policies.
- Advising staff on Data Protection issues and the rules needed to ensure compliance with data protection laws including privacy notices and Data Privacy

Impact Assessments

Providing the Council's (and hence TfC's) point of contact with the Information Commissioner's Office for:

- Consultation on high risk proposals following PIA
- Maintaining arrangements for notification of breaches
- Maintaining notifications to the ICO

10. Staff Roles

10.1 Senior Information Risk Owner

The Senior Information Risk Owner (SIRO) is the Director of Finance and he will take overall ownership of the Organisation's Information Risk Policy, act as champion for information risk on the Board and provide written advice to Chief Executive on internal control in regard to information risk.

The SIRO will assist the organisation to consider the information risks associated with its business goals and how those risks may be managed. The SIRO implements and leads the Information Governance (IG) risk assessment and management processes within the Organisation and advises the Board on the effectiveness of information risk management across the Organisation. The SIRO is responsible for ensuring that organisational information risk is properly identified and managed and that appropriate assurance mechanisms exist.

The Senior Information Risk Owner for TfC is:
Steve Renwick
Director of Finance

10.2 Caldicott Guardian

A Caldicott Guardian is a senior person responsible for protecting the confidentiality of patient and service-user information and enabling appropriate information-sharing. The Guardian plays a key role in ensuring that TfC and partner organisations satisfy the highest practical standards for handling patient identifiable information.

Acting as the 'conscience' of an organisation, the Guardian actively supports work to enable information sharing where it is appropriate to share and advises on options for lawful and ethical processing of information. Their remit covers all health and social care records for children.

As they have responsibilities relating to confidential information and information sharing, the Caldicott Guardians also have a strategic role, which involves representing and championing Information Governance requirements and issues at management team level and, where appropriate, at a range of levels within the organisation's overall governance framework.

The Caldicott Guardian makes sure that where confidential personal information is shared, for example with local NHS or other care partners, this is done properly, legally and ethically in line with the following principles.

The Caldicott Principles are set out at Appendix D.

The overall Caldicott Guardian for Sunderland City Council is:
Fiona Brown
Executive Director of People Services

The Caldicott Guardian for TfC is:
TBA
Principal Social Worker

10.3 Data Protection Officer

The Council has appointed a Data Protection Officer responsible for the statutory duties set out in the data protection legislation, and for the management of the activities of the Data Protection Office

The Data Protection Officer for Sunderland City Council and TfC under a Service Level Agreement is:
Rhiannon Hood
Data Protection Officer
Data Protection Office, Civic Centre, Sunderland, SR2 7DN
E: Data.protection@sunderland .gov.uk
T: 0191 561 0123

10.4 Information Security Manager

The Information Security Manager in conjunction with the Head of Customer Service, Intelligence & ICT has responsibility for assuring the integrity of the Council's Technology Architecture Strategy from a business assurance perspective and provides advice and guidance to and on behalf of customers relating to Information Security and Information Governance standards and implications of technology or

process change on these. This service is again accessed by TfC under a Service Level Agreement

The Information Security Manager for Sunderland City Council is:
Richard Wright

11. Policy Review

11.1 This policy will be reviewed and updated to maintain its relevance annually and recommendations for changes submitted to the Board for approval.

11.2 A copy of the policy in place from time to time will be retained until the end of the period of 6 months beginning on the day processing under that version of the policy ceases in accordance with requirements for processing the special categories of data.

Appendices

Information Charter

Appendix A Related Legislation
Appendix B Caldicott Principles
Appendix C Special Categories of Personal Data
Appendix D Privacy Notices
Appendix E Breach Reporting

Appendix A

Related Legislation

Legislation enforced by Information Commissioner's Office

- Data Protection Act 2018 (DPA);
- General Data Protection Regulation (GDPR);
- Privacy and Electronic Communications (EC Directive) Regulations 20035 (PECR);
- Freedom of Information Act 2000 (FOIA);
- Environmental Information Regulations 2004 (EIR);
- Environmental Protection Public Sector Information Regulations 2009;
- Investigatory Powers Act 2016;
- Re-use of Public Sector Information Regulations 2015;
- Enterprise Act 2002;
- Security of Network and Information Systems Directive (NIS Directive);
- Electronic Identification, Authentication and Trust Services Regulation (e-IDAS).

Other Related Law

- Common Law Duty of Confidence
- The Human Rights Act 1998
- Computer Misuse Act 1990
- The Regulation of Investigatory Powers Act 2000 (RIPA)
- The Telecommunications (Lawful Business Practice) (Interception of
    - Communications) Regulations 2000 (SI 2000/2699)
- The Criminal Justice and Immigration Act 2008
- Protection of Freedoms Act 2012
- Human Rights Act 1998
- European Convention of Human Rights and Fundamental Freedoms
- Health and Social Care Act 2012

Appendix B
Caldicott Principles

The Caldicott principles provide a useful framework for assessing proportionality.

Data controllers must ensure that any restriction of rights is proportionate to the purpose for which the information is shared. In assessing proportionality, the controller should consider the impact on the data subject against the wider benefits of sharing the information. In addition, controllers can only share the minimum amount of information required to achieve the purpose in accordance with the third data protection principle.

1. **Justify the purpose(s)**
   Every single proposed use or transfer of patient identifiable information within or from an organisation should be clearly defined and scrutinised, with continuing uses regularly reviewed, by an appropriate guardian.

2. **Don't use patient identifiable information unless it is necessary**
   Patient identifiable information items should not be included unless it is essential for the specified purpose(s) of that flow. The need for patients to be identified should be considered at each stage of satisfying the purpose(s).

3. **Use the minimum necessary patient-identifiable information**
   Where use of patient identifiable information is considered to be essential, the inclusion of each individual item of information should be considered and justified so that the minimum amount of identifiable information is transferred or accessible as is necessary for a given function to be carried out.

4. **Access to patient identifiable information should be on a strict need-to know basis**
   Only those individuals who need access to patient identifiable information should have access to it, and they should only have access to the information items that they need to see. This may mean introducing access controls or splitting information flows where one information flow is used for several purposes.

5. **Everyone with access to patient identifiable information should be aware of their responsibilities**
   Action should be taken to ensure that those handling patient identifiable information - both clinical and non-clinical staff - are made fully aware of their responsibilities and obligations to respect patient confidentiality.

6. **Understand and comply with the law**
   Every use of patient identifiable information must be lawful. Someone in each organisation handling patient information should be responsible for ensuring that the organisation complies with legal requirements.

7. **The duty to share information can be as important as the duty to protect Confidentiality (Caldicott 2 additional principle)**
   Health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.

Appendix C

Special Categories of Personal Data

Data within the special categories identified at Schedule 1 of the Data Protection Act 2018 will be processed in accordance with this policy and the arrangements set out above to secure compliance with the principles relating to the processing of personal data and retention and erasure of that data.

Data within the special categories will be retained for the periods identified in retention schedules published to the council's internet site www.sunderland.gov.uk

Appendix D

Privacy notices

TfC maintains a central privacy notice setting out in general terms the arrangements for processing.

In complying with the Transparency principle services will provide data subjects with additional privacy information in the form of a privacy notice where this is appropriate to allow the data subject to understand how the data will be processed for the specified purposes.

When preparing a privacy notice services will consider the general guidance provided by the Information Commissioner including the privacy notice checklist;

https://ico.org.uk/media/for-organisations/documents/1625126/privacy-notice-checklist.pdf

When preparing a privacy notice the following information is to be provided in a format appropriate to the service and the data subject's needs.

The pre-populated sections of the privacy notice are also contained in the Council's central privacy notice and it may be appropriate to refer data subjects to that notice for those parts of the information.

PRIVACY NOTICE TEMPLATE 1. (ARTICLE 13)

TO BE PROVIDED AT THE TIME THE DATA IS OBTAINED
FOR USE WHEN THE **DATA SUBJECT** PROVIDES PERSONAL INFORMATION TO TfC

IDENTITY OF DATA CONTROLLER	**TOGETHER FOR CHILDREN**
DATA PROTECTION OFFICER	**DATA PROTECTION OFFICER** **TOGETHER FOR CHILDREN PO BOX 100** **SR2 7DN** **EMAIL:** **Data.Protection@sunderland.gov.uk** **TELEPHONE: 0191 561 1023**
PURPOSES AND LEGAL BASIS FOR PROCESSING	Service to complete
LEGITIMATE INTERESTS (IF APPLICABLE)	Service to complete
RECIPIENTS OF DATA	Service to complete
INTERNATIONAL TRANSFERS INCLUDING SAFEGUARDS	Service to complete
RETENTION PERIOD OR CRITERIA	Service to complete
RIGHT TO REQUEST RECTIFICATION/PORTABILITY/OBJECTION	Your Information Rights are set out in data protection law. you have the right to ask to:

	• have inaccuracies corrected; • have your personal data erased; • place a restriction on our processing of your data; • object to processing; and • request your data to be ported (data portability). Subject to some legal exceptions, we will comply with your request. **To exercise any of these rights please contact the relevant service in the first instance.** You also have the right to request a copy of the personal information we hold about you.
RIGHT TO WITHDRAW CONSENT	Where we process data based on your consent you have the right to withdraw that consent at any time. You can do this by contacting the service direct or through the Data Protection Office
RIGHT TO COMPLAIN TO ICO	If you have concerns about how we have dealt with your personal information, please contact the Data Protection Officer at Data.Protection@sunderland.gov.uk, or by calling 0191 561 1023 You can also contact the Information Commissioner's Office Information Commissioner's Office Wycliffe House Water Lane Wilmslow Cheshire SK9 5AF **Telephone:** 0303 123 1113 (local rate) or 01625 545 745 **Fax:** 01625 524 510
CONSEQUENCE OF FAILURE TO SUPPLY DATA	Service to complete
EXISTENCE OF PROFILING OR AUTOMATED DECISION-MAKING	Service to complete

TO BE PROVIDED AT WITHIN ONE MONTH OF THE DATE THE DATA IS OBTAINED
FOR USE WHEN A **THIRD PARTY** PROVIDES PERSONAL INFORMATION TO TfC

IDENTITY OF DATA CONTROLLER	**TOGETHER FOR CHILDREN**
DATA PROTECTION OFFICER	**DATA PROTECTION OFFICER** **TOGETHER FOR CHILDRENPO BOX 100 SR2 7DN** **EMAIL:** **Data.Protection@sunderland.gov.uk** **TELEPHONE: 0191 561 1023**
PURPOSES AND LEGAL BASIS FOR PROCESSING	Service to complete
CATEGORIES OF PERSONAL DATA OBTAINED	Service to complete
LEGITIMATE INTERESTS (IF APPLICABLE)	Service to complete
SOURCE OF DATA (AND IF APPLICABLE IF IT CAME FROM PUBLICLY ACCESSIBLE SOURCES)	Service to complete
RECIPIENTS OF DATA	Service to complete
INTERNATIONAL TRANSFERS INCLUDING SAFEGUARDS	Service to complete
RETENTION PERIOD OR CRITERIA	Service to complete
RIGHT TO REQUEST RECTIFICATION/PORTABILITY/OBJECTION	Your Information Rights are set out in data protection law. you have the right to ask to: • have inaccuracies corrected; • have your personal data erased; • place a restriction on our processing of your data; • object to processing; and • request your data to be ported (data portability). Subject to some legal exceptions, we will comply with your request. **To exercise any of these rights please contact the relevant service in the first instance.**

	You also have the right to request a copy of the personal information we hold about you.
RIGHT TO WITHDRAW CONSENT	Where we process data based on your consent you have the right to withdraw that consent at any time. You can do this by contacting the service direct or through the Data Protection Office
RIGHT TO COMPLAIN TO ICO	If you have concerns about how we have dealt with your personal information, please contact the Data Protection Officer at Data.Protection@sunderland.gov.uk, or by calling 0191 561 1023 You can also contact the Information Commissioner's Office Information Commissioner's Office Wycliffe House Water Lane Wilmslow Cheshire SK9 5AF **Telephone:** 0303 123 1113 (local rate) or 01625 545 745 **Fax:** 01625 524 510
CONSEQUENCE OF FAILURE TO SUPPLY DATA	Service to complete
EXISTENCE OF PROFILING OR AUTOMATED DECISION-MAKING	Service to complete