

# Bristol City Council - Early Intervention and Targeted Support Privacy Notice

Bristol City Council is the data controller for the purposes of the Data Protection Act 1998 and other regulations including the General Data Protection Regulation (Regulation (EU) 2016/679), which means it determines what your data is used for and why it is collected. The purpose of this privacy policy is to tell you about what information we collect about you when you use our service, how we use that information and who we may share it with.

The contact details of the data controller are **Bristol City Council, City Hall, College Green, Bristol. BS1 5TR.**

Bristol City Council and its partners are committed to working with Children and families and also to meet the Government requirements to deliver the national Troubled families Programme (known Locally as Think Family) in our area. In order to fulfil our obligations it is necessary to share information with critical partners. This is important both for the delivery of the programme and evaluating its effectiveness.

Your privacy is important to us and we take great care to protect it.

## What data we need to collect and the legal basis for processing it:

To provide this service, we have identified the following legal gateways which allow us to process your data for the Think Family programme:

- The Digital Economy Act 2017 and the Public Service Delivery, Fraud and Debt: Data Sharing Code of Practice
- Sections 10 and 11 of The Children's Act 2004,
- Section 82 of The National Health Service Act 2006
- Section 1 of The Childcare Act 2006
- Section 23 and 25 of The Children's and Families Act 2014
- Section 17, 37 and 115 of The Crime and Disorder Act 1998
- Section 11, 21, 157 and 175 of The Education Act 2002
- Section 1 of The Localism Act 2011
- Section 1 of The Children (Leaving Care) Act 2000
- Special Education Needs and Disability Regulations 2014
- Immigration and Asylum Act 1999
- Education and Skills Act 2008 (ESA 2008)

More information can be found at [Bristol City Council Think Family Legal Gateways](#)

## How long we will keep your data for:

The Goddard Enquiry has ruled no data can be deleted from Social Care databases until advised. In order to comply with the National Troubled Families Programme, we are required to retain information from the commencement of the programme in 2014 until 2020.

## Who we share your data with and why:

To understand risk and vulnerability and provide early intervention and targeted support to children and families across the City we may share data with the following recipients:

Partner Agencies such as:

- Commissioned Providers

Educational Providers such as:

- Bristol Schools

Health Services such as:

- Bristol Clinical Commissioning Group (CCG)
- North Bristol Trust (NBT)
- United Hospitals Bristol Trust (UHB)

Emergency Services such as:

- Avon and Somerset Constabulary
- Avon Fire and Rescue

## If we have your consent to use your data:

We rely on statutory duties detailed above and [Bristol City Council Think Family Legal Gateways](#) to process your data, but where we rely on your consent, you can withdraw it at any time.

## What we do with your information:

In order to;

- identify which families need our support
- understand and meet the needs of families
- understand the difference we are making

we will be sharing personal records that relate to you.

This might include records in relation to your social care, any involvement with the police, courts and probation, aspects relating to your employment, anti-social behaviour, violence in the home, substance misuse, educational attendance and behaviour, vulnerable children and health issues.

Our information relating to individuals and families will be matched with information from public agencies and organisations such as the NHS and health organisations, Department of Work and Pensions, the Police, the ministry of Justice, the probation services, schools and Youth offending Team.

We may also give your details to commissioned service providers e.g. a charity that we ask to provide services on our behalf. These commissioned service providers will always have the same security standards as the council.

We may share your information with other councils and other organisations such as our partners in the NHS where this is appropriate.

- Where we rely on your consent you will be told about this or asked to agree to this first, if we decide to share services with these organisations.
- Information shared with our local NHS partners is via a secure system called Connecting Care. [Read more information about this.](#)

This data includes both individuals and families who have been considered to be part of the programme. We may also share your information without asking you if:

- the law says we must.
- there is a risk of serious harm or threat to life.
- we are fulfilling a statutory duty and in order to do so we need to share your personal information.

In addition to this, the national Troubled Families Programme carries out an evaluation in which all local authorities are required to participate. Local authorities are asked to provide the following information:

1. A small amount of personal information (see below for list) for every individual assessed for the programme in order to conduct a National Impact Study (NIS)<sup>1</sup>.

- Personal identifiers of individuals in all families assessed for eligibility (e.g. name, date of birth, gender and postcode)
- Eligibility problems met (as per this Financial Framework)
- Status of intervention (e.g. whether eligible, start/end date of intervention)
- Available unique identifiers (e.g. National Insurance Numbers, Unique Pupil Numbers)

2. Family Progress Data (FPD) every six months for all individuals in families who are being supported by the programme against around a dozen measures for which there are no national administrative datasets. For more information about the Family Progress Data (FPD) please see this [link](#)

## Where we have used automated processing or profiling:

In order to identify risk and vulnerability relating to social issues for children and families we sometimes use automated profiling methods in order to be able to help you access support services.

## Your rights as a data subject:

You have the right to ask for access to your data and where data is found to be inaccurate to have that data corrected. In certain circumstances you have the right to have data held about you erased, or the use of it restricted. You may be able to object to processing, and may also have the right to have your data transferred to another data controller. You have the right to have any inaccurate information corrected. You also have a right of complaint to the Information Commissioner's Office (ICO) at [www.ico.org.uk](http://www.ico.org.uk) if you think we have not dealt with your information in a proper manner. You can ask to see what information we hold about you and have access to it. You can do this, by contacting:

Senior Data Protection Officer  
Bristol City Council  
ICT Commissioning and Information Governance  
P O Box 3176  
BRISTOL  
BS3 9FS  
[Data.protection@bristol.gov.uk](mailto:Data.protection@bristol.gov.uk)

Other questions about the data being processed may also be sent to the above address.

### Fraud Prevention and Detection:

Bristol City Council is required by law to protect the public funds it administers. It may share information provided to it with other bodies responsible for auditing, administering public funds, or where undertaking a public function, in order to prevent and detect fraud. For more information visit <https://www.bristol.gov.uk/data-protection-foi/fraud-prevention-and-detection>

---

i

- the data can only be used for carrying out research;
- the linked data cannot be used to make decisions about individuals;
- the linked information is anonymised to reduce the risk of individuals being identified;
- it will be impossible for any person or family to be identified from any published reports;
- the linked personal data will not be shared with or made available to the local authority or any other public agency;
- all data is transferred, handled and stored in accordance with the Data Protection Act;
- appropriate measures are in place to prevent unauthorised use of the data;
- the data is destroyed after eight years.