BIRMINGHAM CHILDREN'S TRUST

# DATA PROTECTION POLICY

| Version | Date | Summary of Changes | Author/Reviewer |
|---|---|---|---|
| **1.0** | March 2018 | First Issue | Anthony Elliott (Head of ICT & CIO) |
| **1.01** | October 2018 | Review following change in Legislation | Su De (DPO) |
| **1.2** | November 2018 | Various updates | Anthony Elliott (Head of ICT & CIO) |
| **1.3** | February 2020 | No changes | Su De (DPO) |
| **1.4** | May 2021 | Formatting changed for numbering. Section on processing children's data added. | Su De (DPO) |
| **1.5** | November 2023 | Review | Su De (DPO) |
| **1.6** | December 2023 | Review | Su De (DPO) |
| **1.7** | January 2024 | Review and formatting | Su De (DPO) |
| **1.8** | February 2026 | DUAA 2025 alignment: children's higher protection matters, complaints, ADM safeguards, cookies/ technologies, ICO guidance. | Su De (DPO) & IAG Membership |

## CONTENTS

## 1. OVERVIEW AND PUBLICATION PARTICULARS

| | |
|---|---|
| Authority[1] | *Birmingham Children's Trust – Director of Finance and Resources & SIRO.* |
| Owner[2] | *Birmingham Children's Trust – Data Protection Officer* |
| Scope[3] | *As defined in section 3 below.* |
| Review period[4] | *This document will be reviewed at least annually or more often if justified by a change in circumstances.* |
| Related Birmingham Children's Trust documents | *Information Assurance Framework*<br>*Acceptable Use Policy*<br>*Information Risk Register*<br>*Data Breach Process*<br>*These documents are available from the Trust intranet or from the DPO / CIO.* |
| Related Capita ICT & DS documents | *Key Trust security related policies are aligned to Birmingham City Council Policies as the Trust and BCC use shared infrastructure.* |
| Legislation or Regulatory Control references | The relevant legislation is:<br>Article 8 of the European Convention on Human Rights (ECHR),<br>General Data Protection Regulations<br>Data Protection Act 2018, and UK GDPR<br>Common Law Duty of Confidentiality.<br>HMG Security Policy Framework<br>Data Use and Access Act (DUAA) 2025 |

[1] AUTHORITY: The person or organisation who is responsible for enforcing this Policy

[2] OWNER: The organisational position of the person who has rights to authorise changes to, or disposal of, this Policy

[3] SCOPE: The organisations or persons to whom the Policy applies

[4] REVIEW PERIOD: How frequently the Policy should be reviewed

## 2. PURPOSE OF THE POLICY

Data Protection law and guidance is to ensure that individual's rights and freedoms are protected. The Trust is committed to ensuring that the personal data that it holds is used fairly and lawfully in line with the highest standards of ethical conduct.

The Policy supports the Trust in delivering the data protection responsibilities through compliance with the principles set out under UK General Data Protection Regulation: processed fairly, lawfully and in a transparent manner.

Personal data should be:

- used only for limited, specified stated purposes and not used or disclosed in any way incompatible with those purposes.
- adequate, relevant, and limited to what is necessary.
- accurate and, where necessary, up to date.
- not kept for longer than necessary; and
- kept safe and secure.

## 3. SCOPE

This Policy applies to all users of Trust data including employees, contractors, third party employees, agency workers, temporary staff and any third party organisation who has legitimate agreed access to personal data held by BCT or who handle information and personal data held by the BCT, including personal data of our service users, from children and young people, to vulnerable adults and care leavers as well as members of staff employed by the Trust.

### EXAMPLES OF WHERE THIS POLICY APPLIES

- **The Information Asset Owner Role** – The Trust has assigned an Information Asset Owner (IAO) to each service area throughout the organisation for managing personal data and its associated risks.

- **Privacy Notices** – The Trust has published a Privacy Notice on the website, as well as service area specific Privacy Notices and provide timely notices where this is required.

- **Training and Awareness** - The Trust requires all staff to undertake the Trust's required training on data protection and security which must be re-done every year. With certain roles, employees are required to attend additional training identified through the Trust Training Needs Analysis.

  The Trust has an Information Assurance Communication Plan that raises awareness and embeds the culture of privacy and information risks.

- **Incident and Breaches** – The Trust has a reporting mechanism that is communicated to all staff. All reported incidents whether we need to report breaches to the ICO or not are reported, assessed and appropriate action as a part of recovery and containment as well as notification / escalation process.

- **Data Protection Compliance Complaints** – The Trust provides an internal privacy complaints route, allowing individuals to raise concerns with the Trust before escalation to the ICO. Any trends or concerns are reported to the Trust's Information Assurance Group.

- **Information Rights** – The Disclosure Team in the Trust is a dedicated team who manage the information rights process and have clear processes in place to handle including, but not limited to the right to:
  - Be informed with a privacy notice containing certain information about the processing activities;
  - Confirm whether the data controller processes personal data about the data subject and the right to access the personal data processed and obtain certain information about the processing activities (Subject Access);
  - Correct inaccurate personal data (Rectification);
  - Have personal data erased under certain circumstances (Erasure);
  - Restrict the processing of personal data under certain circumstances (Restriction);
  - Receive a copy of the personal data the data controller holds under certain circumstances and transfer the personal data to another data controller (Data Portability);
  - Object to processing of personal data (Right to Object);
  - Not be subject to a decision based solely on automated processing, including profiling (Automated Decisions).

The Trust is under a legal obligation to ensure that the rights of the data subjects are not violated. Data subjects wishing to exercise their rights under data protection legislation should generally make their request. Information on this can be accessed via the Birmingham Children's Trust website.

- **Information Asset Register (IAR) and Records of Processing Activities (ROPA**) – The Trust records all processing activities and the data sharing under these processes in the IAR and ROPA. Where the Trust shares personal information with any third party a 'Data Sharing Agreement' or 'Data Processing Agreement' is put in place as a part of a formally documented written agreement or contract through or in conjunction with the commissioning team.

- **Contracts and Commissioning** - The Trust Commissioning Team oversee that our contracts are compliant with UK GDPR. To ensure an adequate level of protection is applied to personal data 'due diligence' is conducted where appropriate on the other party, and that adequate and appropriate controls and safeguards, including cloud processing and cloud security. Where the Trust and another controller jointly determine why and how personal data should be processed, we will be regarded as a 'joint controller'. The arrangement will reflect the respective roles and relationships of the joint controllers towards the individual(s) and respective Privacy Notices.

- **Cookies** - Cookies and similar technologies ensure appropriate lawful bases/consent and technical controls in line with DUAA, overseen by the CIO and the DPO.

## 4. PROCESSING AND USE OF PERSONAL DATA

The Trust processes personal data to deliver a wide range of services to children and young people as well as employees. These range from safeguarding to employer's responsibilities. The Trust relies on the lawful bases highlighted in the data projection legislations for processing *personal data*:

- consent
- the processing is necessary to comply with our legal obligations (including public duty)
- the processing is necessary to perform a public duty
- the processing is necessary to perform a contract with the data subject
- interest or in the exercise of official authority vested in the Trust
- where not part of the performance of our functions, the processing is necessary for the purposes of legitimate interests pursued by the Trust.

Where the Trust processes *special category data,* (this includes information about racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purposes of identifying an individual, physical or mental health, sex life or sexual orientation), then both a article 6 and article 9 conditions are required.

There are 10 conditions for processing special category data in Article 9 of the UK GDPR. Five of these require you to meet additional conditions and safeguards set out in UK law, in Schedule 1 of the DPA 2018.

a) Explicit consent
b) Employment, social security and social protection (if authorised by law)
c) Vital interests
d) Not-for-profit bodies
e) Made public by the data subject
f) Legal claims or judicial acts
g) Reasons of substantial public interest (with a basis in law)
h) Health or social care (with a basis in law)
i) Public health (with a basis in law)
j) Archiving, research and statistics (with a basis in law)

When the Trust is relying on conditions (b), (h), (i) or (j), checks would be undertaken to ensure that the Trust meets the associated condition in UK law, set out in Part 1 of Schedule 1 of the DPA 2018.

Where the Trust is relying on the substantial public interest condition in Article 9(2)(g), the Trust will ensure that one of 23 specific substantial public interest conditions set out in Part 2 of Schedule 1 of the DPA 2018 is met.

The UK GDPR gives extra protection to the personal data of Criminal Offence Data on offenders or suspected offenders in the context of criminal activity, allegations, investigations, and proceedings. To process personal data about criminal convictions or offences, the Trust must have a lawful basis under article 6 and legal authority or official authority. These are likely to centre on: specific employment requirements; fraud investigations; safeguarding issues; the vital interests of the data subject or other individuals.

**PROCESSING CHILDREN'S PERSONAL DATA**

Children require specific protection with regard to their personal data as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data.

Under the DUAA 2025 s.81, the Trust must evidence that higher protection of children's data matters. This includes considering how best to protect and support children when using our services, that children merit special protection as they may be less aware of risks and rights. and that children will have differing needs at different ages/stages. The Trust conforms to the ICO Children's Code for services likely to be accessed by children.

If the processing involves children's personal data, then the Trust ensures that the bases for processing are compliant when relying on;

- public task / duty
- consent and ensure that the child understands what they are consenting to.
- 'necessary for the performance of a contract'. The Trust will consider the child's competence to understand what they are agreeing to, and to enter into a contract.

- 'legitimate interests'' The Trust will take responsibility for identifying the risks and consequences of the processing, and put age appropriate safeguards in place.

Furthermore, when processing children's data, the Trust ensures that the privacy notices, are child-friendly, clear, risks explained and explaining their rights in a language they can understand. IAOs must ensure DPIAs are updated for age-appropriate design and governance, including proportionate age assurance. Given the Trust's averse risk appetite in social care, residual risks require SIRO sign-off.

More information on Children and the UK GDPR can be found here.

**USE OF CCTV IN THE TRUST**

Closed circuit television cameras (CCTV) is used by the Trust for many reasons, predominantly for the prevention and detection of crime and health and safety. The Trust uses CCTV imagery for the prevention and detection of crime, public safety, to monitor the Trust's buildings in order to provide a safe and secure environment for staff, volunteers, contractors, and visitors, and to prevent the loss of or damage to the Trust's contents and property. The processing of the CCTV imagery in the Trust will in compliance with UK GDPR.

## 5. MONITORING

Compliance with this policy will be monitored via the DPO and Information Assurance reporting to Information Assurance Group (IAG) and Audit Committee.

Unauthorised disclosure of personal data is a disciplinary matter that may be considered a gross misconduct and could lead to termination of employment.

In the case of third parties, unauthorised disclosure could lead to termination of the contractual relationship and in certain circumstances this could give rise to legal proceedings.

Any failure to follow this Policy must be treated as an incident and investigated in accordance with the Trust Breach Management Process.

## 6. SUMMARY

The policy sets out the expected behaviours of Trust Employees and our delivery partners in relation to the collection, use, retention, transfer, disclosure and destruction of any Personal Data relating to an identifiable, living individual.

The Trust follows ICO guidance on DUAA data protection & privacy changes; data protection by design & default (children's higher protection matters); the Children's Code (AADC); ADM & profiling; and Data Protection Complaints.

The standards, process and guidelines that support this Data Protection Policy have been listed on the intranet.

## 7. ROLES AND RESPONSIBILITIES

The Data Protection Policy has been reviewed to ensure that it supports the Information Assurance Framework.

The Senior Information Risk Owner is responsible for administering or enforcing policy.

| Role | Responsibilities |
|---|---|
| The Chief Executive | The Chief Executive is the Trust's Accountable Officer and has ultimate responsibility for compliance with data protection. |
| Information Assurance group | The Information Assurance Group has membership drawn from all departments and directorates to ensure that data protection and information governance is embedded within the organisational structure. IAG is also responsible for endorsing data protection policy |
| SIRO | The SIRO for the Trust is the Director of Resources. The Senior Information Risk Owner is responsible for administering or enforcing policy. |
| Caldicott Guardian | The Caldicott Guardian has overall responsibility for protecting the confidentiality of service user information and enabling appropriate information sharing and hence has a vested interest in the |

| | |
|---|---|
| | policy. The Caldicott Guardian is consulted as a stake holder. |
| CIO | The Chief Information Officer is a key contributor in formulating strategic goals for the Trust in IT. The CIO is consulted as a Stakeholder |
| DPO | The role of the DPO has been set out in the General Data Protection Regulation. The DPO has the responsibility of informing and advising the Trust of obligations under the Data Protection Act 2018 and under the Data protection Policy.<br>The DPO acts as the contact point for the Information Commissioner's Office on issues relating to processing. |
| Information Asset Owners | Information Asset Owners (IAOs) are directly accountable to the SIRO and must provide assurance any personal data processed within the Directorate are compliant with the Data Protection legislation. |
| All Staff | Complete relevant training as required.<br>Promptly report any suspected security incidents or data breaches.<br>Seek advice where they are unsure how to comply with data protection legislation or this policy.<br>Respond promptly to requests from Disclosure Team in connection to data subject rights and freedom of information requests.<br>Understand that failure to comply with Trust policy may lead to disciplinary actions.<br>Understand it is an offence for an individual, knowingly or recklessly, to unlawfully disclose personal data and can lead to personal |

| | |
|---|---|
| | prosecution by the Information Commissioner's Office. |

## 8. EXCEPTIONS

None identified.

## 9. ENFORCEMENT

Any individual member of staff who contravenes this Policy may be investigated under the Trust's disciplinary procedure and, where appropriate, legal action may be taken.

Other individuals within the scope of this Policy may be investigated and, where appropriate, legal action may be taken against them, or withdrawal of privileges. Third parties or partner organisations who contravene this Policy may jeopardise their relationship with Birmingham Children's Trust and may also face legal action.

## 10. APPENDIX

### DEFINITIONS

**Personal Data** - Data/Information that relates to a living individual who can be identified from the data or from any other information that is in the possession of, or likely to come into the possession of the data controller. It includes any expression of opinion and any indication of the intentions of the data controller (or any other person) in respect of the individual.

**Special Categories of Personal** Data – specific categories of personal data which reveal the racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic, biometric and health data of data subjects, and information relating to a data subject's sex life or sexual orientation. These categories are subject to additional processing restrictions.

**Data Controller** - the person or organisation who determines the purposes for which and the manner in which any personal data are, or are to be, processed. The Trust is the data controller in respect of all personal information that relates to Birmingham Children's Trust.

**Data Subject** - is the identified or identifiable person to whom the personal data relates.

**Processing** - is defined very broadly and encompasses collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction (that is, the marking of stored data with the aim of limiting its processing in the future, erasure and destruction. In effect, any activity involving personal data falls within the scope of the GDPR.

**Data Processor** - the person or organisation who processes personal data on behalf of a data controller.