A black text on a white background

Description automatically generated

**Birmingham Children’s Trust**

**Equipment and Data Security Policy**

**Controlled Document**

# Owner: Head of ICT

# Author: Anthony Elliot

Version: 10

Date: December 2024

TABLE OF CONTENTS

* 1. [DOCUMENT CONTROL 3](#_bookmark0)
  2. [Document History 3](#_bookmark1)
  3. [Document Review/Approval/Implementation 4](#_bookmark2)
  4. [Document Sign-off 4](#_bookmark3)
  5. [Document Distribution following Sign-off 4](#_bookmark4)

[2.0 OVERVIEW 5](#_bookmark5)

[3.0 POLICY OBJECTIVES 6](#_bookmark6)

* 1. [POLICY STATEMENTS 7](#_bookmark7)
  2. [Security of equipment 7](#_bookmark8)
  3. [Encryption 8](#_bookmark9)
  4. [Third party access 8](#_bookmark10)
  5. [Data transfer 9](#_bookmark11)
  6. [RESPONSIBILITIES 10](#_bookmark12)
  7. [Service Birmingham Asset Management and Asset Owners 10](#_bookmark13)
  8. [Service Birmingham Facilities 10](#_bookmark14)
  9. [Service Birmingham Heads of Service 10](#_bookmark15)
  10. [Service Birmingham Service Owners 10](#_bookmark16)
  11. [Service Birmingham staff 10](#_bookmark17)
  12. [Third party suppliers 10](#_bookmark18)

[6.0 EXCEPTIONS 11](#_bookmark19)

[7.0 ENFORCEMENT 11](#_bookmark20)

* 1. [APPENDIX – CONTROLS AND RISKS 11](#_bookmark21)
  2. [Control A.10: Cryptography 11](#_bookmark22)
  3. [Control A.11: Physical and environmental security 11](#_bookmark23)
  4. [Control A.13.2: Information transfer 11](#_bookmark24)
  5. [Operation and maintenance 11](#_bookmark25)

# DOCUMENT CONTROL

* 1. Document History

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Summary of Change** | **Agreed By** |
| 0.1 | 08/03/2006 | Initial draft | Mark Grover |
| 0.2 | 02/05/2006 | Revised | Mark Grover |
| 1.0 | 26/05/2006 | Final | Vanessa Stead |
| 1.01 | 19/03/2008 | Review of version 1.0 | Russell Waldron/  Jaspal Sagoo |
| 1.1 | 01/04/2008 | Reformat into new policy template and update following review by Security  Manager | Yvonne Batchelor |
| 2.0 | 01/08/2008 | Following approval from Service  Birmingham Service Management Board | Russell Waldron |
| 2.1 | 21/11/2008 | Review following ISO Audit in Aug 2008 | Russell Waldron |
| 3.0 | 13/02/2008 | Following approval from Service Management Programme Board and BCC  Intelligent Client Function (ICF) Member | Russell Waldron |
| 3.1 | 12/10/2009 | Revisions by Philippa Williams and  Russell Waldron | Philippa Williams |
| 3.2 | 17/02/2010 | Following amendments from the ICF | Dave Thomas and  Caroline Hobbs |
| 4.0 | 19/02/2010 | Following approval from Service Management Programme Board and BCC  Intelligent Client Function (ICF) Member | Russell Waldron |
| 4.1 | 19/12/2011 | Annual Policy Review. Merged policies third party, encryption, data exchange,  equipment. | Jaspal Sagoo/ Russell Waldron |
| 5.0 | 02/02/2012 | Service Birmingham and ICF Sign-off | Jaspal Sagoo |
| 5.1 | 30/08/2013 | Annual review | M. Westrop |
| 5.2 | 12/09/2013 | Changes following review | M. Westrop |
| 6.0 | 26/09/2013 | Following approval from Paul Turnbull | M. Westrop |
| 6.1 | 06/11/2014 | Thoroughly revised and updated | Richard Green |
| 6.2 | 18/11/2014 | Updated following end of review period | Richard Green |
| 7.0 | 25/11/2014 | Following approval from SB senior  management and ICF | Richard Green |
| 7.1 | 03/03/2016 | Reviewed – no changes required | Richard Green |
| 7.2 | 13/02/2017 | Annual review | Richard Green |
| 8.0 | 23/02/2017 | Following sign off | Richard Green |
| 9.0 | 11/12/2023 | Document was overdue for revisions undertaken by Hamant Jakhu | Anthony Elliott |
| 9.1 | 06/09/2024 | Additional revisions following Veritau auditor’s recommendations | Anthony Elliott, BCT Information Assurance Group & Caldicott Guardian |
| 10 | 19/12/2024 | Final sign off, following review of Veritau recommendations | Antony Elliott, Caldicott Guardian (James Burns) |

* 1. Document Review/Approval/Implementation

|  |  |
| --- | --- |
| **Name** | **Service Area** |
| Su De | Data Protection Officer |
| Hamant Jakhu | Senior ICT Manager |
| Anthony Elliott | Head of ICT & CIO |

* 1. Document Sign-off

|  |  |  |
| --- | --- | --- |
| **Name** | **Position** | **Date** |
| Anthony Elliott | Head of ICT & CIO |  |
| James Burns | Caldicott Guardian |  |

* 1. Document Distribution following Sign-off

***NOTE: This document will be distributed only to the following.***

|  |  |
| --- | --- |
| **Name/Group** | **Service Area** |
| All Personnel | Birmingham Children’s Trust |

# 2.0 OVERVIEW

|  |  |
| --- | --- |
| **Purpose** | The purpose of this document is to define the policy rules which govern the security of equipment and data managed by Birmingham Children’s Trust.  Equipment and data must be securely managed to minimise the risk of information loss and the damage associated with losses. |
| **Authority** | Head of ICT |
| **Ownership** | Head of ICT |
| **Scope** | This policy applies to everyone who handles information on behalf of Birmingham Children’s Trust, to the information itself and to all equipment used to process the information. |
|  |  |
| **Review cycle** | This document will be reviewed at least annually. |

# 3.0 POLICY OBJECTIVES

The objectives of this Policy are:

* to ensure that equipment used to process information on behalf of Birmingham Children’s Trust is securely managed.
* to protect the confidentiality, integrity and availability of Birmingham Children’s Trust information assets.
* to specify the requirements for the governance of Birmingham Children’s Trust relationships with its third-party suppliers.
* to set out the rules governing the transfer of data.
* to support compliance with legislative and good practice requirements.

# POLICY STATEMENTS

* 1. Security of equipment

Measures shall be implemented to prevent unauthorised physical access to, damage to or interference with Birmingham Children’s Trusts information and information processing facilities. The following requirements apply.

* Physical security perimeters must be defined and used to protect areas containing information and information processing facilities.
* Secure areas shall be protected by appropriate entry controls. Unauthorised people shall be excluded from the secure areas. Suitable procedures for the management of secure areas must be formulated and applied.
* Appropriate physical security measures shall be applied to offices, rooms and all areas where information processing takes place.
* There must be adequate and appropriate protection against malicious attacks, accidental damage and other external threats.
* Delivery and loading areas, and other places where unauthorised people could enter the premises, shall be controlled. Where possible, such places shall be isolated from information processing facilities.

Measures shall be implemented to minimise the risk of loss or theft or compromise of, or damage to Birmingham Children’s Trusts equipment. The following requirements apply.

* Equipment shall be suitably sited and protected to reduce the risks from environmental threats and hazards and to reduce the opportunities for unauthorised access. Equipment must be sited and used in accordance with health and safety regulations.
* Equipment shall be protected from power failures and from disruption by the failure of supporting utilities.
* Power and telecommunications cabling which carries data or supports information services shall be protected from interception, interference and damage.
* Equipment shall be correctly maintained by suitably qualified engineers.
* Equipment must not be removed from Birmingham Children’s Trusts business premises without management authorisation. Those who remove equipment remain responsible for its security whilst it is off the premises and must take appropriate measures to protect it.
* Movement of equipment and software between Birmingham Children’s Trusts locations must be strictly controlled by authorised personnel.
* Encryption software must be installed and activated on all laptops and portable data storage devices.
* Unattended equipment must have appropriate protection. Users must lock their workstations when they leave their desks.
* Paperwork or removable storage devices containing protectively marked information must not be left unattended on desks.
* Laptops must not be left on desks overnight.
* Any equipment with the capacity to store data must have all sensitive data and licensed software removed or securely overwritten prior to disposal. All equipment must be dealt with in accordance with the requirements of the Birmingham Children’s Trusts Asset Management Procedure.
* Staff must not attempt to install any software on to Birmingham Children’s Trust devices. Any requests for software must be made to the IT Service Desk. The configuration of any Birmingham Children's Trust owned device must not be changed or altered.
* Asset registration numbers must not be removed or defaced. In the event an asset registration number is loose or missing, it must be reported to the IT Service Desk.
* Every effort should be taken to take reasonable care of ICT equipment provided by the Trust.

Further information about the employee’s responsibilities when using IT equipment can be found in the Birmingham Children's Trust Acceptable Use Policy.

* 1. Encryption

Encryption should be used to protect protectively marked information when it is transmitted to external recipients. Prior to transmission, consideration must be given to the procedures to be used by the sending and receiving parties and any possible legal issues from using encryption techniques.

The lending of electronic keys that belong to Birmingham Children’s Trust or its suppliers of ICT services is not permitted.

The management of electronic keys and certificates (used to control the encryption, decryption and signing of sensitive messages) must be performed under dual control, with duties being rotated between authorised Birmingham Children’s Trust or its suppliers of ICT Services staff.

Encryption must not be implemented in such a way that it has an adverse effect on system performance and availability.

AES-256 is the preferred encryption algorithm. Secure Shell (SSH) is the preferred encryption protocol for peer-to-peer encryption. Proprietary encryption algorithms are not allowed for any purpose.

Strong keys, such as Secure Socket Layer (SSL), must always be used when implementing encryption mechanisms.

All written material must be considered as to whether it should be protectively marked, in accordance with the sensitivity of the document.

The main protective marking being used by Birmingham Children’s Trust is **OFFICIAL SENSITIVE** – which will be applied to all information that could have damaging consequences (for individuals or an organisation) if it were lost, stolen or published in the media. An example of this could be personal information, sensitive information and commercially sensitive information.

Any documents that are not protectively marked will be assumed to contain unclassified information that can be viewed in a public domain.

The originator of a document will apply the protective marking. The default protective marking is Official. However, this should be changed if the information within the document becomes sensitive within exchanges (e.g. via email); or a contributor to the document considers the original information should be marked as **OFFICIAL SENSITIVE.**

All information that is produced by Birmingham Children's Trust is subject to FOI (freedom of information) and SAR (subject access requests) whether with or without protective markings,

* 1. Third Party Access

Birmingham Children’s Trust is responsible for the governance of third parties that interact with the company, but it is not responsible for the governance of third parties that interact directly with other organisations (such as Birmingham City Council).

Birmingham Children’s Trust third parties must agree to and sign an Access, Data Sharing or Data Processing Agreement. This agreement covers all aspect of a third party’s interaction with Birmingham Children’s Trust in relation to its access to systems that are managed by Birmingham Children’s Trust or its ICT suppliers.

The SLAM or other equivalent process will be used to create IDs for third parties that have signed agreements. IDs will have a default status of ‘inactive’.

The BCC DTS or other equivalent Change Management process will be used to activate IDs to enable technical support of ICT systems only when they are needed, and to deactivate them once the specific work for which they were activated is completed. The period of activation should be as short as possible.

It is the responsibility of Service Owners to ensure due diligence is conducted to ensure that third parties are reputable. and that they operate in accordance with relevant industry, regulatory and quality standards. Service Owners are also responsible for reviewing the relationships with third party suppliers.

Partner agencies and third-party suppliers must not be given details of how to access Birmingham Children’s Trust network without permission from the Information Assurance Group and the Birmingham Childrens Trust Head of ICT.

The following requirements relate to compliance with Payment Card Industry (PCI) standards.

* Service providers must be PCI DSS compliant.
* Service providers are responsible for the security of the cardholder data they possess.
* The two requirements above must be incorporated into contracts with service providers.
* Any change that affects payment card processing systems must be assessed in terms of its impact on the third party’s PCI DSS compliance status.
* Payment card data must be encrypted when being transmitted.
  1. Data transfer

Data transfers between Birmingham Children’s Trust and third-party suppliers must be managed through the BCC DTS or other equivalent Change Management process. The amount of data transferred should be limited to the minimum necessary to fulfil the purpose of the transfer.

No information that belongs to Birmingham Children’s Trust may be placed on to a portable physical medium unless the information asset owner within the Trust has given written consent.

* 1. Asset Management

Birmingham Children's Trust will ensure the protection of all information assets on its IT estate. The heads of service and team managers are responsible for their team’s information assets as the asset owners.

For the purpose of this policy, “important information assets” for Birmingham Children’s Trust can be identified as, but are not limited to the following:

* Computer Databases and Case Management Systems (CSM)
* Any storage containing paper records
* Data files and folders

Information Asset owners must ensure that:

* All information assets are assessed and classified according to their content
* An access control register is in place for all information assets of which they are the owner (for example, system audit logs and periodic system access reports)
* The asset control register is regularly updated.
* When staff are no longer working for Birmingham Children’s Trust, the asset owner will ensure that all IT equipment is returned from the employee.
* Asset owners will liaise with the ICT Support Team to ensure that access to equipment and systems is revoked/suspended immediately for any employees that are leaving or have been suspended.

# RESPONSIBILITIES

* 1. **Birmingham Children’s Trust ICT**

To ensure that equipment is appropriately managed and protected.

* 1. Birmingham Children’s Trust Facilities

To ensure that equipment usage and placement complies with health and safety and fire regulations.

* 1. Birmingham Children’s Trust Information Asset Owners and Trust ICT

To ensure that encryption is applied appropriately in accordance with this policy. To ensure secret keys used in encryption are managed.

To revoke and amend access requests to systems and equipment as per the starters, leavers and mover’s process.

To have oversight and maintenance of individual asset registers pertaining to their service areas, which records details of equipment, location, user id, manager and current status (ie Live, or Suspended).

To ensure that staff are fully aware and have access to the BCT Acceptable Use Policy.

To ensure that IT equipment is returned from employees no longer working for Birmingham Children’s Trust

* 1. Birmingham Children’s Trust Information Asset Owners

To ensure due diligence is conducted on third party suppliers.

To ensure that ICT asset registers are updated regularly.

To ensure third parties sign an access agreement or data sharing/processing agreement and that it is suitably countersigned by the appropriate Trust Director on behalf of Birmingham Children’s Trust.

To manage the existence and use of third-party IDs through the SLAM and Change Management processes.

To ensure third party supplier relationships are reviewed.

* 1. **Birmingham Children’s Trust Staff**

To safeguard and protect any Birmingham Children’s Trust equipment and data in their care.

To have an appropriate awareness of, and to follow, the rules for the management of third-party access.

To return any IT equipment back to Birmingham Children’s Trust in the event of their employment ending.

* 1. Third party suppliers

To treat Birmingham Children’s Trust information assets with reasonable care and to use appropriate measures to prevent unauthorised access, destruction, corruption or loss.

# 6.0 EXCEPTIONS

There are no exceptions to this policy.

# 7.0 ENFORCEMENT

This policy is mandatory for all permanent, contract and temporary staff at Birmingham Children’s Trust, who are expected to fully comply with its provisions. Additionally, it extends to work placements, students, apprentices, auditors, inspectors, contractors and third-party users.

Birmingham Children’s Trust will perform audits to establish whether policy requirements are being met. Non-conformities will be managed through the Audit and Compliance or Risk Management processes. Any employee found to have knowingly violated this policy may be subject to disciplinary procedures, the sanctions of which may extend to termination of employment.