

Birmingham Children’s Trust ICT Acceptable Use Policy

If you have any enquiries about this policy, please contact Birmingham Children’s Trust Head of ICT & CIO or Data Protection Officer

Version 1.4

Date Classification OFFICIAL

© Birmingham Children’s Trust - December 2024

**CONTENTS**

[1 STATEMENT FROM THE HEAD OF ICT & CHIEF INFORMATION OFFICER 3](#_Toc185521061)

[2 ABOUT THIS DOCUMENT 4](#_Toc185521062)

[2.1 What this document covers and who is affected by it 4](#_Toc185521063)

[2.2 The status of the document 4](#_Toc185521064)

[2.3 How the content is organised 4](#_Toc185521065)

[2.4 Supporting documents 4](#_Toc185521066)

[2.5 Review of the Acceptable Use Policy 7](#_Toc185521067)

[2.6 Document administration data 7](#_Toc185521068)

[3 DEFINITIONS 8](#_Toc185521069)

[4 COMPLIANCE 9](#_Toc185521070)

[4.1 Your responsibilities 9](#_Toc185521071)

[4.2 Security breaches 9](#_Toc185521072)

[4.3 Enforcement action – for people directly employed by the Trust 10](#_Toc185521073)

[4.4 Enforcement action – for people not employed by the Trust 10](#_Toc185521074)

[4.5 Protective action 10](#_Toc185521075)

[4.6 Audit logs, monitoring and privacy 12](#_Toc185521076)

[5 ACCESS CONTROL 13](#_Toc185521077)

[5.1 Control of access to information systems 13](#_Toc185521078)

[5.2 User IDs and passwords 13](#_Toc185521079)

[6 USAGE 15](#_Toc185521080)

[6.1 Use of e-mail and other electronic communications services 15](#_Toc185521081)

[6.2 Use of the Internet 15](#_Toc185521082)

[6.3 Use of the Public Services Network 16](#_Toc185521083)

[6.4 Copyright Adherence 16](#_Toc185521084)

[6.4.1 It is illegal to break copyright protection. Users could break copyright if they download, transmit or copy protected material. 16](#_Toc185521085)

[6.5 General Usage 16](#_Toc185521086)

[Birmingham Children’s Trust IT facilities must not be used in any way that breaks the law or breaches standards. Users must not use Birmingham Children's Trust facilities for: 16](#_Toc185521087)

[6.5.1 Sending threatening, offensive or harassing messages 16](#_Toc185521088)

[6.5.2 Creating or sending obscene material 16](#_Toc185521089)

[6.5.3 Accessing data to which the user is not an intended recipient without permission, even if it is not protected by security controls 16](#_Toc185521090)

[6.5.4 Logging into or attempting to log into any accounts that the user is not expressly authorized to access. 16](#_Toc185521091)

[6.5.5 Executing any form of network monitoring which will intercept data not intended for the user (unless prior authorization has been granted). 16](#_Toc185521092)

[6.5.6 Employees and authorized users of BCT IT equipment are strictly prohibited from accessing unauthorized material, including but not limited to websites, content, or resources that are not related to their job functions or that violates this acceptable use policy and the IT security handbook. 16](#_Toc185521093)

[7 ASSETS 17](#_Toc185521094)

[7.1 Agile working 17](#_Toc185521095)

[7.2 Use of private computer equipment 17](#_Toc185521096)

[7.3 Acceptable use of IT assets 17](#_Toc185521097)

[7.4 Control of software 18](#_Toc185521098)

[8 PROTECTIVE MEASURES 19](#_Toc185521099)

[8.1 Information classification 19](#_Toc185521100)

[8.2 Information protection 19](#_Toc185521101)

[9 LOSSES AND DISPOSALS 20](#_Toc185521102)

[9.1 Information security incidents and personal data breaches 20](#_Toc185521103)

[9.2 Disposal of IT equipment 20](#_Toc185521104)

[10 EMERGING TECHNOLOGIES 20](#_Toc185521105)

[10.1 The only AI (Artificial Intelligence) product authorised for use in the Trust is Microsoft Copilot when running on your work laptop or phone. 20](#_Toc185521106)

[10.2 Copilot should only be used by those engaged with the Trust automation project. 20](#_Toc185521107)

[10.3 No other AI product is authorized for Trust use. 20](#_Toc185521108)

[10.4 Personal devices and any AI products on them must not be used for Trust work 20](#_Toc185521109)

[10.5 Birmingham Children’s Trust handles sensitive personal data, and the use of AI systems may introduce challenges in ensuring full compliance with stringent data protection regulations such as the UK GDPR. 20](#_Toc185521110)

[10.6 AI systems may pose risks if data is processed in ways that are not fully transparent or understood, particularly regarding automated decision making that impacts an individual’s rights. 20](#_Toc185521111)

# STATEMENT FROM THE HEAD OF ICT & CHIEF INFORMATION OFFICER

All of us in Birmingham Children’s Trust (the Trust) use information on a daily basis. We use it as part of providing our services to support the children, young people and families in Birmingham. We also use it to make decisions and carry out the management of the organisation. This information needs to be properly managed for the Trust to operate successfully and meet our legal obligations under the data protection act 2018 and the UK GDPR.

Information exists in a variety of formats, and it is held and processed in a wide range of systems. But regardless of where it comes from, what form it takes or how it is processed, it all needs to be treated securely and with care.

Much of the information we hold has been given to us by citizens and by partner agencies. They have trusted us to keep it safe. If we lose it, or if we don’t protect it properly, we will have failed in our duty.

It is important for everyone to know about the rules and standards that enable us to keep the Trust’s information secure. This policy brings together, in a single document, all the main principles that govern the use of the Trust’s information resources: that is, the information used by the Trust to carry out its business and the systems used to hold and process that information.

This Acceptable Use Policy applies to everyone who has access to the Trust’s information resources. This includes not only those who are directly employed by the Trust: it extends to all who work for or with the Trust to deliver our services and carry out the management of the organisation.

Every individual who is entrusted with any Trust information is personally responsible for securely handling and protecting it. Everyone who uses the Trust’s information has a responsibility for helping to maintain effective security.

No matter where you work, if you use the Trust’s information resources as part of doing your job then this policy applies to you. If you are an employee of the Trust, it is incorporated into the employee code of conduct which forms part of your contract of employment. If you have responsibility for managing others, you are expected to lead by example and to apply these principles yourself as well as requiring your staff to follow them.

It is important for us all to apply the highest professional standards in managing information, this policy will help us to do that, and it is important for you to read, understand and put it into practice.

**Anthony Elliott**

**Head of ICT & Chief Information Officer**

# ABOUT THIS DOCUMENT

## What this document covers and who is affected by it

This document applies to all information held or processed by Birmingham Children’s Trust, or on behalf of the Trust by a third party, and to the systems used to hold and process the information. It applies to everyone who has access to the information or systems: this includes everyone who works for or with Birmingham Children’s Trust, whether employed by the Trust or not.

All third-party vendors, contractors, consultants, and any other external entities (collectively referred to as “third partes”) granted access to Birmingham Children’s Trust’s IT systems, networks or data are required to comply with this IT acceptable use policy. Access is granted solely for the purpose of fulfilling contractual obligations or services agreed upon with the Trust.

Information exists in a variety of formats: it may be electronic, graphic, on microfiche, on film, on audio-tape, printed, hand-written or spoken; and it may be stored on any medium. In this document, the word ‘information’ is intended to refer to the full range of formats and storage media.

## The status of the document

This document is a policy, and it sets out important rules and standards that must be followed by those who use the Trust’s information as part of working for, or with, the Trust. These standards apply all the time: there are no general or automatic exceptions. Any exceptions that might apply or unusual circumstances must be considered on their merits and formally approved by the Trust’s Head of ICT & CIO or Data Protection Officer.

If you are an employee of Birmingham Children’s Trust, you are expected to comply with this policy as it is incorporated into the employee code of conduct. If you are within the scope of the policy but you are not employed by the Trust, compliance is an important condition of your ongoing working relationship with the Trust.

## How the content is organised

The policy has several major sections. Each major section covers a significant topic related to the use of the Trust’s information resources. Within each major section, there is further separation into sub-sections: each sub-section covers different subject matter. Each rule or standard is then explained within the relevant sub-section.

All sections, sub-sections and rules in this document are numbered, so that they can be referred to easily.

## Supporting documents

* + 1. *The Security Handbook*

This ICT Acceptable Use Policy is supported by a Security Handbook.

The Acceptable Use Policy covers all the important rules and standards that apply to all users of the Trust’s information resources. The aim of the document is to bring together, in one place, what you need to know if you use those resources as part of doing your job.

It is written so that you will be able to quickly and easily understand what your obligations are.

* + 1. The Security Handbook contains a more detailed explanation about the rules and standards. It gives practical advice about how they should be applied and implemented. The focus of the Security Handbook is on the promotion of good practice. The advice and guidance it contains is designed to help you to follow the rules and standards. *Procedures, forms and guides*

There are various procedures linked to the ICT Acceptable Use Policy.

In general, a procedure exists to support the implementation of a policy rule. A procedure describes how an activity should be carried out, to achieve a particular result. Some procedures are further supported by guides that contain explanatory notes. There may also be forms that are completed as part of the operation of a procedure.

Whenever a procedure is in place to support a policy rule, this fact is made clear in the Acceptable Use Policy.

* + 1. *The Technical Security Manual*

The Trust has many rules concerning information governance and the operation of systems. Historically, these rules have been explained in a wide range of different documents. For example:

* + - * The standard for the construction of user IDs is set out in the Technical Security Manual.
      * There is a document that explains rules about the development of Microsoft Access Databases.
      * There are rules about access controls that must be considered when an information system is being developed and maintained.

Whilst these rules are important, they do not have a direct effect on the daily work of the majority of people. They apply mainly to defined groups of staff, with specialist job roles, in particular circumstances.

These specialist rules are not described in detail in the Acceptable Use Policy. Instead, they are being incorporated into a Technical Security Manual.

## Review of the Acceptable Use Policy

The content of the Acceptable Use Policy is reviewed on a regular basis. The sections are not all reviewed at the same time as each other.

The footer of each section shows the date when the content of that section was last reviewed.

## Document administration data

The following information about this document is recorded in the version control:

* the history of version date for the document.
* the names of the authors of the document.
* the name of the sign off authority for the document (Head of ICT, Caldicott Guardian and the BCT Information Assurance Group.
* the name of the document owner.
* the name of the authorising body and dates of approval.

This information is available on request from the Head of ICT & CIO

**2.7 Document Version Control**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Version** | **Date of Issue** | **Summary of changes** | **Author** | **Reviewers** | **Organisation** |
| Version 1 | Sept 2018 | First Signed off version | Tony Elliott |  | Birmingham Childrens Trust &  Birmingham City Council |
| Version 1.3 | Sept 2024 | Various updates in the main to reflect changes required because of the UK GDPR coming into effect in January 2021.  Minor changes to definitions and version control included in the document.  Additional information included to emphasise impact of security breaches, reporting protocol, general IT usages and controls around IT disposal. | Hamant Jakhu | Tony Elliott  Caldicott Guardian  BCT – Information Assurance Group | Birmingham Childrens Trust &  Birmingham City Council |
| Version 1.4 | Dec 2024 | Final sign off, after considering Veritau recommendations | Hamant Jakhu | Tony Elliott  Caldicott Guardian | Birmingham Childrens Trust |

# DEFINITIONS

An **information asset** is any data, device, or other component of the environment that supports information-related activities. Assets include hardware (for example, laptops), software and confidential information (for example, a person’s record).

Inappropriate use of information assets exposes Birmingham Children’s Trust and the service users who entrust us with their data to risks.

A **data subject** is a person to whom data relates.

A **data controller** is a person or an organization who alone or jointly determines the purposes and means of the processing of personal data. Essentially the data controller decides **why** and **how** personal data should be processed.

A **data processor** is a person or organization that processes personal data on behalf of the data controller. Birmingham Children’s Trust is a data processor for some organizations such as the NHS and the Police.

A **user of data** is any individual who accesses, uses or interacts with personal data within an organization. This applies to employees, contractors, or other individuals who work with personal data in the course of their duties.

**Personal data** is information relating to an identified or identifiable person (data subject) who can be identified directly and indirectly by reference to an identifier, or specific factors. For example, your name, address and date of birth are examples of your personal data.

**Processing of Data –** refers to any operation or set of operations performed on personal data, whether by automated means or not. The processing of data includes things such as collection, recording, organizing, storing, analyzing, erasing and the destroying of data.

**NDA –** Non-Disclosure Agreement

**BCT –** Birmingham Children’s Trust

**CIO** - Chief Information Officer is the individual within the organization responsible for the management, implementation and usability of information and computer technologies.

**DPO** – Data Protection Officer is the individual within Birmingham Children Trust who monitors internal compliance and advises on data protection obligations.

**PC -**means any personal computer device such as a tablet, laptop or desktop.

**Mobile -**means any Smart Mobile Device that is portable with a mobile network voice or data connection, including smart phones, standard phones, tablets or portable devices such as printers and ticket reading devices. Note that some tablet devices (for example, a tablet with a mobile network connection) fall into both the PC and mobile category and rules for both must be followed.

**BYOD -** Bring Your Own Deviceis the practice of allowing employees to use their own computers smartphones and other devices for work purposes.

# COMPLIANCE

## Your responsibilities

* + 1. If you use the Trust’s information resources as part of doing your job, then the rules and standards described in this policy apply to you. They apply not only to those who are directly employed by the Trust, but to all who work for or with the Trust to carry out its business.
    2. Everyone who works for or with the Trust has a duty of confidentiality and a responsibility to safeguard the Trust’s information. Every individual who is entrusted with any Trust information is personally responsible for securely handling and protecting that information.
    3. If you use the Trust’s systems or equipment, then you must do so in an acceptable way.
    4. Everyone who uses the Trust’s information and systems has a responsibility for helping to maintain effective security.

## Security breaches

* + 1. If you do not follow the rules and standards contained in this Acceptable Use Policy, then the Trust’s information could be put at risk. Information might be lost or might become known to people who have no right to know it. If this happens, it will be classed as a security breach.
    2. Security breaches can have a wide range of consequences. Some examples of these consequences are listed below.
       - If personal information about the Trust’s service users is released inappropriately, those people could suffer embarrassment or distress or could be put in danger.
       - If information becomes corrupted or if it is not available when needed, the Trust might not be able to deliver essential services.
       - If a breach involves information shared between the Trust and an external partner, the relationship with the partner organisation could be seriously damaged.
       - The Trust’s finances could be affected by a breach. The Information Commissioner has the power to impose substantial, multi-million-pound fines for data protection breaches. In addition, the Trust could be at an increased risk of fraud or theft from those who seek to gain unauthorised access to its systems.
       - The Trust could suffer significant damage to its reputation because of the publicity surrounding a breach.
    3. If a security breach occurs because of something you have done, or have failed to do, then you may be held accountable for your behavior and actions. The consequences of the security breach may be directly attributed to you. This means that you could be held responsible for any loss of or damage to the Trust’s information and for any financial losses resulting from the breach.
    4. In the event of a data breach, you have a duty to report it to the DPO and your manager without delay to minimise the impact. This may involve securing the affected systems and preventing further unauthorized access.

## Enforcement action – for people directly employed by the Trust

* + 1. This Acceptable Use Policy is incorporated into the employee code of conduct which forms part of your contract of employment. This means that you are required to comply with it as part of your conditions of employment.
    2. If you do not comply with the rules in the Acceptable Use Policy, then disciplinary action may be taken against you. This could result in you being dismissed from your job, particularly if you have committed gross misconduct.
    3. If you do not comply with the rules then, in addition to disciplinary action, you could also face legal proceedings.
    4. If there is evidence that you have committed a criminal offence through your use of the Trust’s systems or equipment, the police will be informed, and you could be prosecuted.

## Enforcement action – for people not employed by the Trust

* + 1. If you do not comply with the rules in the Acceptable Use Policy, then your access to the Trust information resources may be removed. The Trust may withdraw your access without telling you in advance.
    2. The way in which you use the Trust’s information resources is reflected on the organisation for which you work. If you do not follow the rules or if you misuse those resources, the Trust may review its existing relationship with your organisation. In some cases, the Trust might take action for breach of contract, or it might terminate the contract with your organisation altogether.
    3. If you work for another organisation and you do not comply with the rules, then your employer may take disciplinary action against you. You, as an individual, or the organisation for which you work, could also face legal proceedings.
    4. If there is evidence that you have committed a criminal offence through your use of the Trust’s systems or equipment, the police will be informed, and you could be prosecuted.
    5. BCT may terminate contracts or agreements with third parties involved in any data breaches, particularly if the breach results from non-compliance with contractual data protection obligations.
    6. BCT may opt to include clauses for financial penalties or compensation for damages resulting from any data breaches.

## Protective action

* + 1. The Trust may use any reasonable methods to protect its information resources. It may take actions in defined situations, to control or reduce the effects of

non-compliance with the rules in this Acceptable Use Policy. These actions are in addition to the enforcement action described above.

* + 1. There are certain well-established protective actions that apply in specific situations. These are made clear at the appropriate points in this document.

## Audit logs, monitoring and privacy

* + 1. In general, your use of the Trust’s computer systems must be related to your work. Private or personal use of the Trust’s systems is not allowed, apart from limited “personal use” of e-mail and the Internet.
    2. Computer systems generally keep records of all user activity in audit log files. The contents of log files may be examined or investigated to establish whether the rules and standards in this policy are being followed.
    3. Section 5.1.1 of the Security Handbook tells you about “personal use” of the e-mail system it explains:

1. how you should label personal e-mails; and
2. how you should file personal e-mails, if you choose to keep them in your mailbox; and
3. the circumstances in which your e-mails (including personal e-mails) could be disclosed.
   * 1. Section 5.2.1 of the Security Handbook tells you about “personal use” of the Internet at work. It explains:
4. that all use of the Internet at work (including personal use) is automatically recorded; and
5. the circumstances in which information about your use of the Internet (including personal use) could be disclosed.
   * 1. You can have some expectation of privacy in relation to “personal use” of e-mail and the Internet at work, but not complete privacy. If you wish to avoid having this sort of personal information recorded and the possibility of having it disclosed, you may choose to:
6. use your own private e-mail account for matters that are not related to work; and
7. use your own private equipment and Internet connection to access the Internet.

# ACCESS CONTROL

## Control of access to information systems

* + 1. You must use the appropriate procedures, such as SLAM and RUC, to manage people’s access to systems.
    2. If you want to access information that is in another person’s account, you must use the appropriate procedure (Investigation Access or Emergency Access). Data access for investigative/emergency purposes will only be granted to authorized individuals who have a legitimate need to know, and those individuals will be subject to these access controls so BCT can maintain an oversight to prevent misuse or unauthorized access.
    3. You must not make any attempt to take control of another person’s account.
    4. You must not allow other people to use your own access to systems.
    5. Special rules apply to administrator accounts. You are not allowed to use this type of account without special permission.
    6. BCT staff should not work with personal data that is about individuals known to them on a personal basis, e.g. family, neighbours, friends, acquaintances. If there is a known conflict of interest this should be flagged to the relevant team manager at the earliest opportunity.

## User IDs and passwords

* + 1. Any personal IDs and passwords issued to you are for your use only. You must not share your personal passwords with anyone else under any circumstances.
    2. You must not ask other people to share their personal passwords with you or with each other. The ICO has the power to impose multi million pound fines, if it has just cause to feel that BCT have had a personal data breach due to negligence.
    3. You must not knowingly attempt to gain access to a compromised account. BCT may face legal actions from affected individuals or groups, which can lead to court proceedings and additional financial liabilities.
    4. Wherever possible, you must use a strong password rather than a weak one. A strong password should be a minimum of twelve characters long, the password should also contain at *least one* character from the following groups which are lower case letters, upper case letters, digits and symbols (further guidance can be found within the BCT – Setting strong passwords document).

Not all of the Trust’s computer systems support the use of strong passwords (legacy systems). If you cannot use a strong password, you must use one that is as good as it can be in the circumstances.

* + 1. Certain types of passwords are automatically weak, and you must not use them.
    2. If a system prompts you to change your password, then you must do so at the earliest opportunity. You should not use passwords that you have used in the recent past.
    3. Special rules apply to file passwords. Access to this type of password must be carefully managed and controlled.
    4. A breach of data security can be defined to an event where personal data is compromised through any of the following incidents:
       - Data Loss & Inaccessibility – The loss of unavailability of personal data where data is unintentionally or unlawfully destroyed, deleted, or rendered inaccessible.
       - Unauthorized Access/Disclosure – The unauthorized access, viewing, or disclosure of personal data, where the access is gained by individuals or entities who are not permitted to view or use the data.
       - Loss of Integrity – The iteration, corruption, or unauthorized modification of personal data, resulting in data that is inaccurate or unreliable, and which may impact its accuracy or usability.

For more information and advice about all of the points in this section, see the Security Handbook.

# USAGE

## Use of e-mail and other electronic communications services

* + 1. If you use the Trust’s electronic communications services, you must accept that they are provided to support the Trust’s business activities.
    2. You must appreciate the security risks associated with e-mails and other electronic communications. You must always be careful not to expose the Trust’s systems and information to unnecessary risk.
    3. Any information that you exchange in electronic communications must be protected in an appropriate way.
    4. You must not use the Trust’s electronic communications services to participate in any kind of criminal or unlawful activity.
    5. You must not use the Trust’s electronic communications services in a way that wastes resources or causes unnecessary disruption or inconvenience to anyone else.

## Use of the Internet

* + 1. If you use the Trust’s Internet service at work, you must accept that the service is provided to support the Trust’s business activities.
    2. You must appreciate the security threats that the Internet presents and be careful not to expose the Trust’s systems and information to unnecessary risk.
    3. The Internet service at work is provided for business use. You must accept that there are restrictions on what you are allowed to look at, whenever you use the Internet at work.
    4. You must not use the Internet at work to participate in any kind of criminal or unlawful activity.
    5. You must not use the Internet at work in a way that breaches any of the Trust’s policies or causes unnecessary disruption.
    6. If you use social media websites, you must be aware of the risks involved and you must be careful about what you publish.

For more information and advice about all of the points in this section, see the Security Handbook.

## Use of the Public Services Network

* + 1. Before you access the Public Services Network (PSN), you must understand what it is and what your obligations are.
    2. Whenever you access the PSN, you must do so only within the Trust, only for conducting Trust business, and using only your own account.
    3. Whenever you deal with information within the PSN, you must protect it appropriately.
    4. You are personally responsible for helping to maintain effective security in the PSN.

## Copyright Adherence

## It is illegal to break copyright protection. Users could break copyright if they download, transmit or copy protected material.

Users must not:

* + 1. Transmit copyright software from their PC or allow any other person to access it from their PC unless the license permits this.
    2. Knowingly download or transmit any protected information/material (including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources and copyrighted music) that was written by another person or organisation without getting permission.
    3. Copy/install copyright software from/to their PC for any purpose not approved by the Trust and for which the user does not have an active license.
    4. Transmit software, technical information, encryption software or technology, in violation of international or regional export control laws.

## General Usage

## Birmingham Children’s Trust IT facilities must not be used in any way that breaks the law or breaches standards. Users must not use Birmingham Children's Trust facilities for:

## Sending threatening, offensive or harassing messages

## Creating or sending obscene material

## Accessing data to which the user is not an intended recipient without permission, even if it is not protected by security controls

## Logging into or attempting to log into any accounts that the user is not expressly authorized to access.

## Executing any form of network monitoring which will intercept data not intended for the user (unless prior authorization has been granted).

## Employees and authorized users of BCT IT equipment are strictly prohibited from accessing unauthorized material, including but not limited to websites, content, or resources that are not related to their job functions or that violates this acceptable use policy and the IT security handbook.

# ASSETS

## Agile working

* + 1. Managers are responsible for deciding whether agile working arrangements are beneficial and appropriate.
    2. If you take part in agile working, you are responsible for protecting the information and the equipment that you use.

## Use of private computer equipment

* + 1. Trust employees are not allowed to use personal computer equipment for Trust business unless explicitly authorised by the Head of ICT & CIO or Data Protection Officer on a case-by-case basis.

## Acceptable use of IT assets

* + 1. You must not attempt to modify or interfere with the Trust’s computer equipment.
    2. The information that you have access to at work is provided to enable you to do your job. It must not be used for other purposes.
    3. You must not use the Trust’s IT and electronic communications equipment to support your private business interests or other employment.
    4. You must not store private documents and files on the Trust’s computer equipment.
    5. You must not use the Trust’s computer equipment to take part in harassment, bullying or other inappropriate behaviour.

For more information and advice about all of the points in this section, see the Security Handbook.

## Control of software

* + 1. All software is managed by BCC, DTS Digital Technology Services or the appropriate suppliers. You must not make any attempt to install, modify, transfer, copy or remove any software yourself unless explicitly authorized by Trust ICT.
    2. You are responsible for helping to protect the Trust’s systems against malicious software.
    3. All smart mobile devices will be managed by the Mobile Device Manager. Attempts to breach this will be monitored centrally by the remote Mobile Device Management Software
    4. Trust applications and logins should not be downloaded onto personal smart mobile devices (BYOD) unless explicitly authorised by Trust ICT on a case-by-case basis.

# PROTECTIVE MEASURES

## Information classification

* + 1. All information that you deal with at work is classified into one of three categories:

1. NOT PROTECTIVELY MARKED; or
2. OFFICIAL; or
3. OFFICIAL–SENSITIVE.

You must understand what these categories mean.

* + 1. Some information, but not all, must be marked with its security classification. You must know when this marking needs to take place, and how to do it.

## Information protection

* + 1. There are four basic principles that govern the protection of the Trust’s information. They are:

1. value and protection.
2. personal responsibility.
3. need to know.
4. exchange.

You must understand these principles and what they mean in practice.

* + 1. All information has value and needs to be protected in an appropriate way.
    2. Everyone who works for or with the Trust has a duty of confidentiality and a responsibility to safeguard the Trust’s information. Adherence to this acceptable use policy is paramount which outlines specific criteria to be followed in ensuring the Trust data is always protected, which will safeguard data transit internally and externally.
    3. Access to sensitive information must be granted only on the basis of a genuine “need to know”.
    4. When information is exchanged with others outside the Trust, it must be protected.
    5. You are responsible for storing information securely.
    6. You must be careful not to allow unauthorised access to information.
    7. If you transfer information to a portable device, you must protect it properly.
    8. You must understand the rules that apply whenever you exchange information with others.
    9. You should understand that there are various methods of information transfer and know when to use them.

# LOSSES AND DISPOSALS

## Information security incidents and personal data breaches

* + 1. You must understand what information security incidents and personal data breaches are and be able to recognise an incident or breach that has occurred.
    2. If you know about an information security incident or a personal data breach, you must report it as soon as you can.
    3. You must co-operate fully with any investigation into an information security incident or a personal data breach.

## Disposal of IT equipment

* + 1. If you need to dispose of IT equipment, it must be handed over to the ICT Support Team who will arrange secure disposal.
    2. If you are a third party who uses BCT IT equipment as part of your agreed role. Upon completion of the agreed work the Trust IT equipment must be handed back to the ICT Support Team, who will arrange inspection and redistribution of equipment.

# EMERGING TECHNOLOGIES

# The only AI (Artificial Intelligence) product authorised for use in the Trust is Microsoft Copilot when running on your work laptop or phone.

# Copilot should only be used by those engaged with the Trust automation project.

# No other AI product is authorized for Trust use.

# Personal devices and any AI products on them must not be used for Trust work

# Birmingham Children’s Trust handles sensitive personal data, and the use of AI systems may introduce challenges in ensuring full compliance with stringent data protection regulations such as the UK GDPR.

# AI systems may pose risks if data is processed in ways that are not fully transparent or understood, particularly regarding automated decision making that impacts an individual’s rights.

For more information and advice about all of the points in this section, see the Security Handbook.