INFORMATION TECHNOLOGY SECURITY POLICY

Approving Body	Trust
Date of Last Review	December 2023
Statutory (Y/N)	N
Responsible Officer	BMAT CEO for and on behalf of the Trust

(ICT) Security Policy for Beacon Multi-Academy Trust

Including

- **Acceptable Use of Computers (Annex 1)**
- **ICT Resource Procedure (Annex 2)**
- **Staff Laptop Procedure (Annex 3)**

1. Introduction

1.1 In all areas of work across the trust, the use of ICT is vital and must be protected from any form of disruption or loss of service. It is therefore essential that the availability, integrity and confidentiality of the ICT systems and data are maintained at a level that is appropriate for our needs. We are investing significantly in ICT facilities across the trust.

1.2 Sufficient resources should be allocated each year to ensure the security of the schools' ICT systems and to enable users to comply fully with the legal requirements and policies covered in this Policy. If insufficient resources are available to fully implement this policy, then the potential risks must be documented and reported to Senior Management.

2. Policy Objectives

2.1 Against this background there are two main objectives of the ICT Security Policy:-

a) to ensure that equipment, data and staff are adequately protected on a cost-effective basis against any action that could adversely affect the school;

b) to ensure that users are aware of and fully comply with all relevant legislation;

2.2.1 If difficulties arise in the interpretation and/or appreciation of any aspects of the Policy, the IT helpdesk, or Trust Manager should be consulted.

3. Application

3.1 The ICT Security Policy is intended for all Trust staff who have control over or who use or support the schools' administration and curriculum ICT systems or data. Students using the schools' ICT systems or data are covered by the relevant **'Acceptable Use of Computers'** and **'The ICT Statement of Policy'** documents, which are incorporated within this policy.

3.2 For the purposes of this document the terms `ICT' (or `ICT system'), `ICT data' and 'ICT user' are defined as follows:-

- `ICT' (or `ICT system') means any device for automatic storing and processing of data and includes central computer, minicomputer, microcomputer, personal computer, mobile devices (whether hand- held laptop, portable, stand-alone, network or attached to a central computer), workstation, word-processing system, desk top publishing system, office automation system, messaging system or any other similar device;
- `ICT data' means any information stored and processed by ICT and includes programs, text, pictures and sound;

- 'ICT user' applies to any Beacon Multi-Academy Trust employee, pupil or other authorised person who uses the schools' ICT systems and/or data.

4. Scheme of Delegation under the ICT Security Policy

4.1 The ICT Security Policy relies on management and user actions to ensure that its aims are achieved. Consequently, owner, corporate and individual levels of responsibility for ICT security are clearly defined below.

4.2 Owner

4.2.1 The owner has the legal title to the property. In this respect, all software, data and associated documentation produced in connection with the work of the school are the legal property of the Beacon Multi-Academy Trust, which will normally hold it for the benefit of the schools.
Exceptions to this will be allowed for software and documentation produced by individual teachers for lesson purposes – this includes schemes of work, lesson plans, worksheets or as otherwise agreed in writing by the Accounting Officer.

4.2.2 We also use software and data that are the legal property of external organisations and which are acquired and used under contract or licence.

4.3 Trust

4.3.1 The Trust has ultimate corporate responsibility for ensuring that the schools comply with the legislative requirements relating to the use of ICT systems and for disseminating policy on ICT security and other ICT related matters.

In practice, the day-to-day responsibility for implementing these legislative requirements rests with the Trust Executive

Trust Executive

4.4.1 They are responsible for ensuring that the legislative requirements relating to the use of ICT systems are met and that the schools' ICT Security Policy, as may be amended from time to time, is adopted and maintained by the school. He/she is also responsible for ensuring that any special ICT security measures relating to the school's ICT facilities are applied and documented as an integral part of the Policy.

In practice, the day to day functions should be delegated to the 'Network Team'.

4.4.2 The Trust Executive are also responsible for ensuring that the requirements of the Data Protection Act 2018 are complied with fully by the school. This is represented by an on-going responsibility for ensuring that the:-

- Registrations under the Data Protection Act are up-to-date and cover all uses being made of personal data and
- Registrations are observed with the school.

4.4.3 In addition, the Trust Executive are responsible for ensuring that users of systems and data are familiar with the relevant aspects of the Policy and to ensure that the appropriate controls are in place for staff to comply with the Policy. This is particularly important with the increased use of computers and laptops at home. Staff should exercise extreme care in the use of personal data at home to ensure legislation is not contravened, in particular the Data Protection Act 2018.

4.5 Network Team

4.5.1 The 'Network Team' is responsible for the school's ICT equipment, systems and data and will have direct control over these assets and their use, including responsibility for controlling access to these assets and for defining and documenting the requisite level of protection. The System Management and leadership of all school network teams is contracted to an external IT Services company by Beacon Multi-Academy Trust.

4.5.2 Consequently, the Network Teams will administer the practical aspects of ICT protection and ensure that various functions are performed, such as maintaining the integrity of the data, producing the requisite back-up copies of data and protecting the physical access to systems and data.

4.5.3 In line with these responsibilities, the external IT services company will be the official point of contact for ICT security issues and as such is responsible for notifying the Trust Executive of any suspected or actual breach of ICT security occurring within the school. The Trust Executive should ensure that details of the suspected or actual breach are recorded and made available to Internal Audit upon request. The Trust Executive must advise Internal Audit of any suspected or actual breach of ICT security pertaining to financial irregularity.

4.5.4 It is vital, therefore, that the Network Teams are fully conversant with the ICT Security Policy and maintain an up-to-date knowledge of best practice and follow the associated approved practices.

4.6 Users

4.6.1 All users of the schools ICT systems and data must comply with the requirements of this ICT Security Policy, the relevant rules of which are summarised in *`Acceptable Use of Computers', ' ICT Resource Procedure', and '(ICT) Statement of Policy'* attached in Annexes A1 – A3.

4.6.2 Users are responsible for notifying the Network Team of any suspected or actual breach of ICT security – the Headteacher/Principal should be informed at the same time. The Headteacher/Principal will discuss with the network team, and support on appropriate follow-up. If a data breach has occurred, the DPO will be informed.

The Legislation

5.1 Background

5.1.1 The responsibilities referred to in the previous sections recognise the requirements of the current legislation relating to the use of ICT systems, which comprise principally of:-

- Data Protection Act 2018;
- Computer Misuse Act 1990;
- Copyright, Designs and Patents Act 1988
- Communications Act 2003

This is not a comprehensive list, and other laws, policies and licences may apply

5.1.2 It is important that all staff are aware that any infringement of the provisions of this legislation may result in disciplinary, civil and/or criminal action.

5.1.3 The general requirements arising from these acts are described below.

5.2 Data Protection Act 2018

5.2.1 The Data Protection Act exists to regulate the use of computerised information about living individuals. To be able to meet the requirements of the Act, the Trust Executive are required to compile a census of data giving details and usage of all relevant personal data held on computer within the school and file a registration with the Data Protection Registrar. It is important that amendments are submitted where the scope of the system extends to new areas of operation. The 2018 Act is consistent with the principles established in the 1984 Act, but extends the regulation to certain manual records as well as computerised information.

5.2.2 It is important that all users of personal data are aware of, and are reminded periodically of, the requirements of the act and, in particular, the limitations on the storage and disclosure of information.

5.2.3 Failure to comply with the provisions of the prevailing Act and any subsequent legislation and regulations relating to the use of personal data may result in prosecution by the Data Protection Registrar.

5.3 Computer Misuse Act 1990

5.3.1 Under the Computer Misuse Act 1990 the following are criminal offences, if undertaken intentionally:-

- Unauthorised access to a computer system or data;
- Unauthorised access preparatory to another criminal action;
- Unauthorised modification of a computer system or data.

5.3.2 All users must be given written notice that deliberate unauthorised use, alteration, or interference with a computer system or its software or data, whether proprietary or written 'in-house', will be regarded as a breach of school policy and may be treated as gross misconduct and that in some circumstances such a breach may also be a criminal offence.

5.4 Copyright, Designs and Patents Act 1988

5.4.1 The Copyright, Designs and Patents Act 1988 provides the legal basis for the protection of intellectual property which includes literary, dramatic, musical and artistic works. The definition of 'literary work' covers computer programs and data.

5.4.2 Where computer programs and data are obtained from an external source they remain the property of the originator. Our permission to use the programs or data will be governed by a formal agreement such as a contract or licence.

5.4.3 All copying of software is forbidden by the Act unless it is in accordance with the provisions of the Act and in compliance with the terms and conditions of the respective licence or contract.

5.4.4 The Network Team is responsible for compiling and maintaining an inventory of all software held by their School and for checking it at least annually to ensure that software licences accord with installations. To ensure that we comply with the Copyright, Designs and Patents Act 1988 and in order to satisfy Beacon Multi-Academy Trust, users must get prior permission **in writing** from the Trust before copying any software.

5.4.5 The Network Team is responsible for compiling and maintaining an inventory of all software held by their school and for checking it at least annually to ensure that software licences accord with installations.

5.4.6 All users must be given written notice that failure to comply with the provisions of the Act will be regarded as a breach of school policy and may be treated as gross misconduct and may also result in civil or criminal proceedings being taken.

5.5 The Communications Act 2003

5.5.1 The Communications act 2003, section 127, makes it an offence to send "indecent, obscene or menacing character over a public electronic communications network"

The Telecommunications Regulations 2000 impose restrictions on the interception of communications such as e-mail.

6. Management of the Policy

6.1 The Trust Executive should allocate sufficient resources each year to ensure the security of the school's ICT systems and to enable users to comply fully with the legal requirements and policies covered in this Policy. If insufficient resources are available to fully implement this policy, then the potential risks must be documented and reported to the Trust.

6.2 Suitable training for all ICT users and documentation to promote the proper use of ICT systems will be provided. Users will also be given adequate information on the policies, procedures and facilities to help safeguard these systems and related data. A record of the training provided through the schools to each individual user should be maintained.

6.3 In addition, users will be made aware of the value and importance of such ICT systems and data, particularly data of a confidential or sensitive nature, and be made aware of their personal responsibilities for ICT security.

6.4 To help achieve these aims, the relevant parts of the ICT Security Policy and any other information on the use of particular facilities and techniques to protect the systems or data will be disseminated to users.

6.5 The Trust Executive must ensure that adequate procedures are established in respect of the ICT security implications of personnel changes. Suitable measures should be applied that provide for continuity of ICT security when staff vacate or occupy a post. These measures as a minimum must include:-

- a record that new staff have been issued with, have read the appropriate documentation relating to ICT security, and have signed the list of rules;
- a record of the access rights to systems granted to an individual user and their limitations on the use of the data in relation to the data protection registrations in place;
- a record that those rights have been amended or withdrawn due to a change to responsibilities or termination of employment;

Physical Security

7.1 Location Access

7.1.1 Adequate consideration should be given to the physical security of rooms containing ICT equipment (including associated cabling). As far as practicable, only authorised persons should be admitted to rooms that contain servers or provide access to data. The server rooms should be locked when left unattended.

7.1.2 The Network Team must ensure appropriate arrangements are applied for the removal of any ICT equipment from its normal location.

7.2 Equipment Siting

7.2.1 Reasonable care must be taken in the siting of computer screens, keyboards, printers or other similar devices. Wherever possible, and depending upon the sensitivity of the data, users should observe the following precautions:-

- devices are positioned in such a way that information stored or being processed cannot be viewed by persons not authorised to know the information. Specific consideration should be given to the siting of devices on which confidential or sensitive information is processed or retrieved;

- equipment is sited to avoid environmental damage from causes such as dust & heat;
- users have been instructed to avoid leaving computers logged-on when unattended if unauthorised access to the data held can be gained. Clear written instructions to this effect should be given to users;
- users have been instructed not to leave hard copies of sensitive data unattended on desks;

The same rules apply to official equipment in use at a user's home.

7.3 Inventory

7.3.1 The Trust Executive, in accordance with the Trust's Financial Regulations, shall ensure that an inventory of all ICT equipment (however financed) is maintained and all items accounted for at least annually.

Annex 1 - Acceptable Use of Computers Policy

1. Background

This policy for acceptable use of computers has been written by the Trust, building on Government guidance. It has been agreed by the Trust and LGBs. It will be reviewed annually.

2. Reasons for making computer facilities available in schools

The purpose of computer use in the schools is to raise educational standards, to promote student achievement, to support the professional work of staff and to enhance the school's management information and business administration. Computer use is part of the statutory curriculum and a necessary tool for staff and students.

The Internet is an essential element in 21st Century life for education, business and social interaction. The Trust has a duty to provide students with quality Internet access as part of their learning experience.

3. Use of computer equipment

Access to up-to-date computer equipment is a key part of the ethos of the Trust and a major benefit to students and staff. All users should appreciate the cost and value of this resource and treat it with appropriate respect. Careless or deliberate action causing equipment damage will result in disciplinary action, which may include loss of access privileges and charges for repair or replacement.

4. The Internet

4.1 Use of the Internet to enhance learning

The Internet offers the following educational benefits:

- access to online educational resources including homework, revision and exam-based resources
- staff professional development through access to national developments, news, exam board resources, educational materials and good curriculum practice
- communication with support services, professional associations and colleagues
- exchange of curriculum and administration data with the Local Authority (LA) and Department for Education (DfE)

Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of students.

Staff will guide students in online activities that will support the learning outcomes planned for the students' age and maturity.

Students will be educated in the effective use of the Internet in research, including the skills of knowledge location and retrieval.

Students will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Students will be taught to acknowledge the source of information and to respect copyright when using Internet material in their own work.

Training will be available to staff in the evaluation of Web materials and methods of developing students' critical attitudes.

A log of all network users internet usage are stored and periodically monitored by the Network Teams for inappropriate usage.

Access to the internet is provided purely for the benefit of Learning and Teaching. It is not acceptable to use this resource for personal benefit.

Internet use is monitored and filtered, and any inappropriate material is blocked and raised with the safeguarding teams.

In common with other media some material available via the Internet is unsuitable for students. The Trust and schools will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The Trust cannot accept liability for the material accessed, or any consequences of Internet access.

4.2 Risk assessment

The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.

Methods to identify, assess and minimise risks will be reviewed regularly.

4.3 Access management

All Internet access will be monitored.

If staff or students discover unsuitable sites, the URL (address) and content must be reported to the BMAT IT Service Desk.

The Network Team will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Any material that the Trust and schools believes is illegal must be referred to the appropriate authorities.

4.4 Social Media (and chat websites)

Students will not be allowed access to public or unregulated chat rooms. Access to social networking websites are strictly prohibited to all users.
(**Selective staff may be allowed temporary access for investigative purposes**). Newsgroups will not be made available unless an educational requirement for their use has been demonstrated.

4.5 BMAT websites available externally

The point of contact on the website will be the school address, school e-mail and telephone number. Staff or students' home information will not be published. Website photographs that include students will be selected carefully and will not enable individual students to be identified.

Students' full names will not be used anywhere on the website, particularly associated with photographs.

Written permission from parents or carers will be obtained before photographs of students are published on the Trust and school websites.

The Trust has overall editorial responsibility and will ensure content is accurate and appropriate.

The website should comply with the Trust's guidelines for publications.

The copyright of all material must be held by the Trust or schools, or be attributed to the owner where permission to reproduce has been obtained.

5. E-mail

All users are provided with an email account purely for educational or business use for the benefit of Beacon Multi-Academy Trust. Personal or inappropriate use of this resource is strictly prohibited. Students may only use approved e-mail accounts on the school systems. Access in the schools to external personal e-mail accounts is be blocked.

Students must not send and should immediately tell a member of staff if they receive offensive e-mail. **The forwarding of chain letters is banned.**

Students should not reveal details of themselves or others, such as address or telephone number, or arrange to meet anyone in e-mail communication.

E-mail sent to an external organisation should be written carefully and checked before sending, in the same way as a letter written on BMAT or school headed paper. The following disclaimer is appended to all external e-mails.

> ***"The contents of this e-mail are confidential and may be privileged, and are intended only for the use of the person or company named herein. Any views or opinions presented are solely those of the author and do not necessarily represent those of Beacon Multi-Academy Trust. If you are not the intended recipient of this e-mail or a person responsible for delivering it to the intended recipient, you are hereby notified that any distribution, copying or dissemination of the information herein is strictly prohibited."***

6. Information stored on BMAT computer systems

All users are personally responsible for anything they store on BMAT computer systems. Storage or distribution of offensive material will result in disciplinary action.

The Trust reserves the right to monitor the content of all files stored on its systems. Staff who operate monitoring procedures will be supervised by senior management.

6.1 Data Protection

Remote access to the Trust and schools' resources are provided to all users with restricted access

where necessary. Users are responsible for the safe usage and security of their login details. Users must not leave themselves logged in unattended at any time. Access for all staff is provided over secure VPN which does not require files from the Trust network to be stored remotely.

Any file required for remote storage should be appropriately encrypted with technology provided by the Trust.

Use of removable storage e.g. USB sticks, and removable hard drives will not be permitted on the Trust network without full acceptance of our security procedures. All removable storage must be encrypted as per our Acceptable Use of Computers Policy.

6.2 Mobile Device Access

Access to Beacon Multi-Academy Trust network resources is limited when using smart mobile devices e.g. phones, iPads, or any other mobile device. Mobile devices are only permitted with the full acceptance of the Trust network security procedures.

6.3 Remote Storage Service

The Trust does not support public unregulated storage services such as Dropbox or any other remote storage that cannot be audited by security auditors. Access to such resources is blocked by our security systems.

7. Communication of this Policy

7.1 Staff

All staff including teachers, supply staff, classroom assistants and support staff, will be provided with this document and its importance explained.
The process of logging onto the Trust's computer system will include agreement to abide by this policy.
Staff development in safe and responsible computer use and on the application of this policy will be provided as required.

7.2 Students

Rules for responsible computer use will be posted near all computer systems. Students will be informed that computer use will be monitored.
Instruction in responsible and safe use should precede Internet access.
The process of logging on to the Trust's computer system will include agreement to abide by this policy.

7.3 Parents

Parents' attention will be drawn to this policy in newsletters and on the Trust and school websites.

A partnership approach with parents is encouraged. This will include demonstrations, practical sessions and suggestions for safe Internet use at home.

Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be made available to parents.

A stock of relevant leaflets from organisations such as BECTa, PIN and NCH Action for Children

will be maintained.

8. Dealing with issues/concerns

Parents and students will need to work in partnership with staff to resolve issues. Responsibility for handling incidents will be delegated to a senior member of staff. Any complaint about staff misuse must be referred to the appropriate member of the Trust Executive.

There may be occasions when the Police must be contacted. Early contact could be made to establish the legal position and discuss strategies.

Sanctions available include:

- follow up/sanction by Head of Year
- informing parents or carers
- removal of Internet or computer access for a period, which could prevent access to school work held on the system, including examination coursework
- charges for damage caused by carelessness, negligence or deliberate misuse of equipment.

Annex 2 - Staff ICT Resource Procedure

This ICT resource procedure is a supplement of the Trust ICT Security Policy

The Trust has allocated Staff the use of ICT equipment such as laptops, iPads, and/or other ICT related accessories to use offsite in order to enhance, enrich, and facilitate Learning and Teaching. These resources are to be used as a productivity tools for school-related business, research, curriculum enhancement, and communication

This procedure supplement applies to the use of all ICT resources inside and/or outside the Trust premises. Staff members are expected to follow all of these ICT procedures when using the Trust ICT resources.

All ICT related resources are property of the Trust and are provided to Staff members for a period of time deemed appropriate. As a condition of the use of these resources, Staff members must agree and comply with all of the following:

1. Prior to being issued with any ICT resource, Staff members must sign the appropriate Procedure Form and agree to all outlined procedures.
2. Staff member issued with any ICT resources is responsible for its use and care during and after the end of business.
3. ICT resource must not be used by any other individual except the Staff member to whom it is assigned.
4. Staff member must not install any software or change the system configuration in any way.
5. It is expected that Staff members will protect any ICT resource from theft or damage.
6. Upon the Trust request, Staff members will provide immediate access to any ICT equipment that have been assigned for their use or care by the Trust.
7. If ICT resource is lost, damage, or stolen, the Trust must be notified immediately.
8. Failure to return the Trust ICT resource will be considered a breach of this agreement, and as such the Trust will take any necessary action to recover the cost of its property.

Annex 3 – Staff laptop Acceptance Form

I understand that all equipment and/or accessories the school has provided to me are the property of Beacon Multi-Academy Trust. I agree to all of the terms in this procedure form. I will return the equipment in the same condition in which it was provided to me. I understand I am personally responsible for any damage that might occur from non-school related or due to user negligence. I understand that I am personally and financially responsible for the lost or theft of any laptop and/or related accessories that has been provided to me. I will not install any additional software or change the configuration of the equipment in any way. I will not allow any other individual to use the laptop and/or related equipment that has been provided to me by Beacon Multi-Academy Trust. I understand that the terms and condition set out in this broad procedure will result in the restriction and/or termination of the Trust computer system and/or accessories

I accept full responsibility for the safe and secure handling of this laptop

Signature_____

Print Name_____