Bury St Edmunds All-Though Trust

Information Technology Policy

Horringer Court Site

Approved by:	[Adam Wilkinson]	**Date:**	[01/11/18]
Last reviewed on:	[November 2018]		
Next review due by:	[November 2019]		

Contents

1 Aim

The aim of Bury All-Through Trust is to provide an excellent education in a healthy, safe, supportive learning environment, where people are valued and make positive contributions to the School community, and where students enjoy and achieve and go on to attain social and economic well-being as responsible, independent members of society.

The policy outlines the commitment of the students, staff and Governors to promote equality. This involves tackling the barriers which could lead to unequal outcomes so that there is equality of access and the diversity within the School community is celebrated and valued.

We believe that equality at our School should permeate all aspects of School life and is the responsibility of every member of the School and wider community. Every member of the School community should feel safe, secure, valued and of equal worth. At Bury All-Through Trust, equality is a key principle for treating all people the same irrespective of their gender, ethnicity, disability, religious beliefs/faith tradition, sexual orientation, age or any other of the protected characteristics (Equality Act 2010).

2 Principles

Staff and students at Bury All-Through Trust have the right to work and study using the IT Services provided by the School in a safe and secure learning environment. Access to these resources must also conform to current UK and international laws.

3 Purposes

The policy defines and describes the use of the IT network and electronic information to support, enhance and develop all aspects of the curriculum and beyond at Bury All-Through Trust in a safe and supportive environment. This document complements and refers to the School Online Safety Policy as well as sections of the Child Protection and Safeguarding Policy.

4 Objectives and Scope

The primary objectives of this policy are:

- To safeguard IT resources and the integrity of data stored on them;
- To minimise the liability arising from the misuse of IT resources and data;
- To ensure that the confidentiality of data is protected to the extent allowed or required by all laws pertaining to it;
- For the benefit of this policy, “IT Estate” will include, but not limited to, all connected devices to the IT infrastructure, software (inc licences), storage devices, telephony (fixed and mobile) and electronic communication.

5 School Responsibilities

The IT Estate is the property of Bury All-Through Trust.

We will ensure that all users are fully aware of the contents contained within this policy. This information will be transmitted to staff through the staff handbook as well as the staff user agreement. New staff also have an IT induction as part of their induction process.

When a breach of this policy is reported, the incident will initially be reviewed by the IT Services Manager and where appropriate either the School Business Manager or escalated to the Principal. If necessary, it will be passed to the appropriate authority.

Within the terms of the Data Protection Act 1998, Human Rights Act 1998 and the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, the School may record or inspect any information transmitted through or stored within its IT Estate. This will be done where;

- There is reasonable cause to believe the user has violated or is violating this policy, any guidelines or procedures established to implement this policy;
- An account appears to be engaged in unusual or unusually excessive activity;
- It is necessary to do so to protect the integrity, security, or functionality of IT Estate or to protect the School from liability;
- Preventing, detection of crime or any other otherwise required by the law;
- Investigating or detecting unauthorised use of the IT Estate;
- Ensuring effective operation of IT Estate.
- For business continuity purposes

6 User Responsibilities

When using any part of IT Estate, all users must comply with all laws pertaining to their access, including copyright, libel, fraud, discrimination and obscenity laws.

By logging onto or using any part of the IT Estate belonging to the School, the user agrees to abide by this policy as well as the other policies that concern use of IT within the School including Online Safety Policy.

Staff and students must be aware that all data including electronic email and documents stored on the system may be accessible to the public under the Freedom of Information Act 2000.

All users are to ensure that their logon details are not shared with any other user. This includes password(s), usernames or any other identifiable credentials, such as photocopier PINs.

Users should make sure that they “lock” their computer (inc laptop) when they are away from their desk & that no part of the IT Estate is left unsecure. It is everybody’s responsibility to ensure that the IT Estate that they interact with is left secure when not in use.

Portable items should be kept secure at all times.

Data stored on any removable media is the responsibility of the user and any personal information (information about staff, students, parents, etc.) must be securely stored. Any data lost (ie on removable devices, laptops, etc.) must be reported to IT Manager or the School Business Manager immediately who will contact the DPO.

No person may knowingly:

- Copy, save or redistribute copyright-protected material, without approval, this includes music & video files;
- Connect a device to the network or any IT resource without prior approval from IT Services;
- Play online computer games or use interactive ‘chat’ sites unless specifically approved by the School;
- Retrieve, send, copy or display offensive, pornographic, obscene or racist messages or pictures.
- Use obscene or racist language, or harass, insult or attack other people.
- Damage computers, computer systems or computer networks.
- Knowingly corrupt or destroy other users’ data.
- Knowingly introduce or attempt to introduce a "virus".
- Attempt to bypass network or computer security including Antivirus Software, using programmable scripts or network monitoring software.
- Attempt to gain access to or use resources NOT allocated to them.
- Download programs/applications without approval of IT Services.
- Use Peer to Peer file sharing programs (Kazaa, Emule, BitTorrent, etc.).

Users should:

- Inform IT Services or an appropriate member of staff if they believe that attempts have been made to use the internet in an unacceptable manner.
- Inform IT Services or an appropriate member of staff if they discover any materials they consider may be offensive or inappropriate.
- Inform IT Services if they damage or discover damaged IT equipment.

7 Appropriate Use of Email

Email provided by the School is to be used in for the teaching, learning, research and School operations. Email should not be used:

- For personal use
- For the transmission of unsolicited commercial or advertising material, chain letters, press releases, or other junk-mail of any kind.
- For the transmission of confidential material concerning the activities of the School
- For the transmission of material such that this infringes the copyright or including intellectual property rights

8 Preventing the Spread of Malicious Software (Viruses)

Users of School IT facilities must take all reasonable steps to prevent the receipt and transmission by email of malicious software e.g. computer viruses in any way that contravenes current UK and international law.

9 Internet Content Filtering

The School takes all possible steps in ensuring that the content of the internet is filtered by use of technology and is appropriate for the needs of the School. The web content filtering solution has full support from the manufacturer and never goes out of support when in service.

All users should be aware that IT Services can and does track and record the sites visited and the searches made on the network by individual users.

If a student or member of staff is unfortunate enough to access any inappropriate web pages, whilst using School equipment, they should make a note of the address, switch off the monitor and report it to the IT Manager or Student Support Manager immediately. The device should not be touched or left unattended. IT Services will then take the appropriate action.

10 Additional Guidelines

IT services will review files and communications to maintain system integrity and ensure that users are using the system responsibly. While normal privacy is respected and protected by password controls, users must be aware that all information stored on the network can be accessed by IT Services and any individual as deemed by the Principal.

11 Discovery of Incidents Involving Illegal Materials or Activities

These should be reported to IT Services or an appropriate member of staff immediately. Please refer to the Online Safety Policy for further guidance.

12 Backups

All servers are backed up in accordance to the backup procedure. A copy of this is available from the IT Manager as well as being included in the Business Continuity Plan.

13 IT Disaster Recovery

Full Disaster recovery procedures are contained within the School Business Continuity Plan. Further information on this is available from the IT Services Manager.

14 Disclaimers

The School arranges for an appropriate disclaimer to be appended to all email messages that are sent to external addresses from the School, in order to provide necessary legal protection. The current disclaimer reads as:

"This email and any files transmitted with it are confidential and intended solely for the use of the individual or entity to whom they are addressed. If you have received this email in error, please notify the system manager. Please note that any views or opinions presented in this email are solely those of the author and do not necessarily represent those of Bury All-Through Trust. The recipient should check this email and any attachments for the presence of viruses. Bury All-Through Trust accepts no liability for any damage caused by any virus transmitted by this email."

15 Legal Consequences of Misuse of Email Facilities

Users must be aware that if they contravene laws relating to the use of email they may be subject to legal proceedings.

16 Investigation of Complaints

The School will investigate complaints in line with the School complaints policy. Please refer to this for further guidance.

17 Telecommunications

The School conducts business by telephone. It is important, therefore, to ensure that the telephone system is used appropriately. It is also important to minimise call charges. The School is keen to ensure that telephone contact with stakeholders is conducted in a professional and efficient manner.

Personal Telephone Calls

School staff should not make personal telephone calls during working hours. However, there may be emergency situations where it is necessary for members of staff to make a brief private call. Staff should use their own mobile phone to make and receive calls unless it is an emergency where use of the School telephones is permitted.

It is not acceptable for staff to conduct regular, private or personal business or administration using the School telephone. Any such abuse of the telephone system could result in disciplinary action.

Staff should also note that they are expected to ensure that incoming personal telephone calls are also kept to a minimum and are of short duration.

Any questions about the appropriateness or regularity of personal calls should be directed to the School Business Manager. The telephone system is a School resource and use of the telephone can and may be monitored. An itemised list of telephone numbers called which states the originator extension and time of call can be produced at any time.

Mobile Telephone Calls

Staff issued with a School mobile phone should use their phone for business purposes only, unless in a personal emergency. Where a mobile phone is used for personal reasons, calls should be logged so that an appropriate charge can be made to the person concerned.

The School allows staff to bring in personal mobile phones and devices for their own use. Members of staff should not contact a student or parent using their personal device.

Students are allowed to bring personal mobile devices/phones to school but must hand them in at the start of the day and must not use them within lesson time. Please refer to the Behaviour Policy.

18 Breaches of the Code (including breaches of security)

Any breach of the Policy by School staff will be initially investigated by the IT Services Manager. The School Business Manager and Principal may also be involved depending on the nature of the breach.

Any serious breach of the Policy will be immediately investigated and an independent investigation carried out to make recommendations on how to remedy the breach.

19 Social Networks

Access to Social Networks, such as Facebook, Twitter etc will only be allowed for School purposes. Staff should not access these sites for personal reasons.

Staff should not “friend” or “follow” students on social networks. Please refer to the Online Safety Policy & the Acceptable User Agreement form for further information

20 Disposal of Redundant IT Estate

All redundant IT Estate will be disposed of through an authorised agency. This should include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data.

All redundant IT Estate that may have held data will have the storage media over written multiple times to ensure the data is destroyed. Or if the storage media has failed it will be physically destroyed. Any IT Estate that is due to be disposed of is stored securely in an independently alarmed & keyed room with no external access.

- We will only use authorised companies who will supply a written guarantee that this will happen Disposal of any IT equipment will conform to: The Waste Electrical and Electronic Equipment Regulations 2006
- The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007
- Data Protection Act 1998
- Electricity at Work Regulations 1989

The School will maintain a comprehensive inventory of all its IT equipment including a record of disposal.

The disposal record will include:

- Date item disposed of
- Authorisation for disposal, including verification of software licensing
- Any personal data likely to be held on the storage media
- How it was disposed of eg waste, gift, sale.
- Name of person and/or organisation who received the disposed item

Please refer to the Asset Security Policy for further guidance.

21 Zombie Accounts

Zombie accounts refer to accounts belonging to users who have left Bury All-Through Trust and therefore no longer have authorised access to the School's systems. Such Zombie accounts when left active can cause a security threat by allowing unauthorised access.

- All user accounts, staff and student will be disabled once they have been taken off role;
- Staff data will be held for one month and then deleted;
- Student data will be deleted annually in January

22 Servers

Details of who has the authority to access servers

- Servers will always be kept in a locked and secure environment with limited access rights.
- Servers will always be password protected.
- Existing servers should have security software installed appropriate to the machine's specification.
- Data must be backed up regularly.

Related Policies

This policy should be read alongside the School's policies on:

- Data Protection/GDPR
- Online Safety
- Child Protection and Safeguarding
- Disciplinary Procedures
- Finance
- Acceptable Use Agreement