Bosworth Independent College

# USE OF ICT, e-SAFETY AND INTERNET ACCEPTABLE USE POLICY (STUDENTS)

| | |
|---|---|
| Updated | September 2021 |
| Review Date | September 2022 |
| Lead Staff for Review | Principal |

# Contents

## Purpose

The purpose of this policy is to ensure that all students studying any educational programme at Bosworth Independent College or online are fully conversant on the acceptable usage policy governing accessing and use of any and all ICT Services at the college.

This policy includes but is not limited to Bosworth provided IT facilities, Internet services and methods of accessing these services together with the use of any and all connected peripheral devices whether provided by Bosworth or by students directly.

This policy ensures the management of personal data, information, security and use of computers within the college are framed by UK, EU and US legislation and is subject to the appropriate monitoring framework to ensure compliance with the following legislation

UK Legislation:

- UK Data Protection Act 2018.
- Regulation Of Investigative Powers Act (2000)
- Freedom Of Information Act (2000)
- Human Rights Act (1998)
- PREVENT Duty guidance (2015)
- Counter-Terrorism and Security Act 2015.
- Payment Card Industry (PCI) compliance.
- Children Act 1989
- Safeguarding children and young people (Children Act 2004)
- Safeguarding Vulnerable Groups Act 2006
- Children and Young Persons Act 2008
- ISI (Independent Schools Inspectorate) Regulations
- Computer Misuse Act (1990)
- Telecommunications Act (1984)
- The Telecommunications Regulations 2000
- Obscene Publications Act (1959)
- Protection of Children Act (1978)
- Defamation Act (1996)

EU Legislation

- The EU 1995 Directive on personal privacy.

USA Legislation

- Health Information Privacy (HIPAA)
- Family Educational Rights and Privacy Act (FERPA)
- Information Technology Law
- Section 508 of the Rehabilitation Act

It aims to ensure that these IT facilities are used effectively for their intended purpose without infringing legal requirements or creating unnecessary risk.

Any breach of these conditions may lead to withdrawal of the user's access to Bosworth provided ICT facilities. A breach of these conditions will lead to an appropriate level investigation and in some instance could lead to criminal prosecution.

## General Principles

The provisions of this policy apply to **all** digital devices used to access Bosworth IT provided facilities, this includes mobile phones, tablet machines, iPads, laptops, PCs, Macs and any other device attached to Bosworth networks regardless of whether they are supplied by the educational establishment or owned by the Student.

All users must demonstrate a responsible approach towards the use of the resources available to them including the use of portable storage items (such as laptops, mobile phones and memory sticks) and their interface with local ICT facilities. They must show consideration to other users and those with whom they come into contact on the Internet, by email or in person.

Use of the Internet and associated facilities are intended for education purposes. However, Boarding house Students will be permitted to play games and watch DVD's in the evenings or times when College lessons are not happening. The Residential Managers will determine the appropriateness of the material and filtering systems will be in place.

Any user of Bosworth provided IT systems must not create, access, transmit or download inappropriate or extremist materials, or contravene any of the said legislation, using Bosworth or any facility or partner associated with Bosworth IT systems or network. Bosworth has a statutory duty to take steps to prevent individuals being drawn into extremism and terrorism, and a duty to alert and report any attempted access to, or dissemination of, such inappropriate material.

## Use of Resources

The College's personal computers must only be used to access the Internet through an officially authorised route.

The user should only download, print, transmit and/or store essential resource material and should always check that the length of a document is reasonable before printing, and wherever possible print in black and white only.

The user must maintain the confidentiality of all user IDs, passwords and other credentials provided by the College. They must under no circumstances be disclosed to any individuals outside the college, and should remain confidential within the college unless the student is specifically requested to divulge them by an authorised member of Staff.

## Unacceptable Deliberate Use/Misuse of ICT Resources

The following activities, whilst not an exhaustive list, are unacceptable:

- Access to, or creation, transmission or publication of, any obscene or indecent, racist, extremist or otherwise offensive images, sounds, data, emails or other material.

- Access to, posting or commenting on of any such materials on an internet based service, including but not limited to blogs, wikis, chatrooms, bulletin boards or any other social media.
- Access to, or creation, transmission or publication of, any data capable of being displayed or converted to such obscene or indecent, racist, extremist or otherwise offensive images, sounds, data or other material.
- Access to, creation, transmission, commenting on, or publication of any material which is designed or likely to cause offence, inconvenience or needless anxiety.
- Creation, transmission or publication of defamatory material.
- Receipt or transmission of material such that this material infringes the copyright of another person or organisation, or which infringes the conditions of the Data Protection Act 1984.
- Accessing, transmission or creation or publication of material that contravenes the Counter-Terrorism and Security Act 2015
- Transmission of unsolicited commercial or advertising materials to other users within the College, users of the Internet or any other network accessible via the Internet.
- Download and/or installation of any unauthorised software onto College equipment.
- Posting anonymous messages and forwarding chain letters
- Using the network for personal gain, for promoting political views or for any form of personal advertising.
- Deliberate damage to College IT equipment or theft thereof.
- Deliberate unauthorised access to facilities, services, data or resources at the College or any other network or service accessible via the Internet
- Deliberate attempts to attack, overload or deny normal operational use of any services, data or resources at the College or any other network or service accessible via the Internet
- Deliberate activities intended to misrepresent or hide the student's identity, or otherwise disrupt, avoid or circumvent any of the colleges' security, access or content control technologies.
- he use of any file sharing, peer to peer (P2P) or "torrent" based services or software.
- The use of any software which is not fully and lawfully licenced for use on the appropriate equipment.
- Falsify, create, modify or distribute any materials that mis-represents official college communications.
- Deliberate activities with any of the following characteristics or which, by their nature, would result in :
- Wasting staff or other users' efforts or network resources, including time on remote systems, bandwidth or the efforts of staff involved in the support of those systems.
- Corrupting or destroying other users' data.
- Violating the privacy of other users.
- Disrupting the work of other users.
- Using the Internet in a way which denies service to other users by overloading the connection to the network or by downloading large files without prior consultation with the IT Systems Administrator.
- Continuing to use any item of software after being requested to cease its use because it is disrupting the correct functioning of College systems or the Internet.

- The introduction or design of computer viruses, Trojans or other malware.

Any use of the Internet that would bring the name of the College into disrepute.

## Monitoring

At any time and without prior notice the College maintains the right and ability to examine any systems and inspect and review any and all data recorded in those systems and any associated storage whether local, portable or internet based. Any information stored in a computer/phone/memory stick or other device may be subject to scrutiny by the College. This examination helps ensure compliance with internal policies and the law.

Students will be required to provide all credentials, passwords and encryption keys to facilitate such an examination, refusal to so will be regarded as a severe breach of this policy.

Where there are grounds for suspecting that a student or students may have, or may be, accessing improper material on the College's ICT resources or their personal equipment, then:

a) The Principal, Vice-Principal, Global Head Of IT or any authorised member of the College management team may request the ICT Support staff to investigate, and require the student to provide any necessary credentials.

b) ICT Support staff will issue a report as soon as practical to the Principal

c) ICT Support Staff shall store any materials so found in an appropriate and secure manner, keeping the number of copies required to the minimum

d) In cases where the material could lead to a criminal offence, the management team shall take appropriate legal guidance on which external authorities should be involved.

In order to ensure compliance with this policy, the College may employ monitoring software to check on the use and content of use of the Internet so as to ensure that there are no serious breaches of the policy. The College specifically reserves the right for authorised personnel to access, retrieve, read and delete any communication that is created on, received through or sent in association with use of the Internet and portable storage facilities to ensure compliance with College policies. Such monitoring will be used for legitimate purposes only.

## Use of Personal Equipment by Students.

Students may use their own digital equipment to enhance their education experience and facilitate communications with their parents or guardians, however students must adhere to the following policies and responsibilities. Any use of personal equipment is at the discretion of the college.

- Student equipment may not be directly connected to a wired network point in student houses & accommodation. Students are not permitted to connect personal equipment to any wired networks within the colleges, classroom, cafeteria or any other college location.
- Students may connect to clearly designated college Guest or Student wireless networks only.
- Students are expected to maintain appropriate, up to date, AntiVirus, Anti Spam and Anti Malware software on any machine they connect to College networks.