Version: 1
Date: September 2023
Next Review: September 2024
Responsibility: John Wilson (Principal)

Brampton College ICT Acceptable Use Policy

Introduction

Brampton College recognises that access to technology in college gives students greater opportunities to learn, engage, communicate and develop skills that will prepare them for work, life and Further Education. We are committed to helping students develop 21st-century technology and communication skills. To that end, we provide the privilege of access to technologies for student and staff use.

This Acceptable Use Policy outlines the guidelines and behaviours that all users (staff, students and contractors who access the college's IT services on college owned and personally owned devices) are expected to follow when using College technologies or personally-owned devices on site, including:

- The Brampton College network is intended for educational purposes
- All activity over the network and use of technologies may be monitored and stored in line with our Information and records retention policy
- Access to online content via the network may be restricted in accordance with our policies and government regulations

Technologies Covered

This Acceptable Use Policy applies to College-owned and personally-owned devices that access the College network and Internet.

The Internet is provided for students for purposeful educational use (e.g. to conduct research or communicate with others on educational matters).

Individual users of the Internet are responsible for their behaviour and communications over the network. Student computer storage areas will not be confidential. Staff may review files and communications to ensure that users are using the system responsibly.

As new technologies emerge, Brampton College will seek to provide access to them. The policies outlined in this document cover all available technologies now and into the future, not just those specifically listed or currently available.

Usage Policies

Students will be assigned a username and password when they arrive but their account will remain disabled until the **Student Acceptable Use Agreement Form** has been received by the College Office.

Once a network account has been activated, students can facilitate personally-owned devices for Internet access by connecting to the College Wi-Fi network.

In the event of ICT resources being used to access networks or systems outside of Brampton College, it is expected that Acceptable Use Policies as set out by the organisations concerned are also observed.

The college uses the Smoothwall monitoring system which analyses conversations and media being shared from College-owned and personally-owned devices while using the College network. This monitoring enables the college to target key issues that affect children, young people and adults and helps us meet safeguarding and e-safety obligations. We recognise the duty of care towards the young people and adults we work with and the need to safeguard these individuals against the risks of cyberbullying, sexual abuse, drugs, mental health, self-harm, radicalisation and more.

At the same time, the College's policy in this area recognises that many children now have unlimited and unrestricted access to the internet via mobile phone networks (i.e.,3G, 4G, and 5G), which some of them may abuse to sexually harass

their peers, share indecent images consensually and non-consensually and view and share pornography and other harmful content. The College undertakes to educate students about and to protect them from the dangers of such activities through raising staff awareness, for example in the ONS Safeguarding course, along with assemblies, PT activities and PSHE lessons.

Further information on Smoothwall can be found here: https://uk.smoothwall.com/markets/education/

User's Digital Rights

We believe that rules and sanctions do not help us become safe users of technology. Therefore the College community agree to enable the following rights to ensure we all have a positive and safe online lifestyle:

- I have the right to enjoy the Internet and all the informative, fun and safe things it has to offer within College boundaries and rules.
- I have a right to keep information about myself private. I only have to tell people what I really want them to know in conversation and profiles.
- I have a right to explore the Internet but I know that I cannot trust everything that I see or read on the Internet and will be discerning in how I use this information.
- I have a right to know who I am talking to on the Internet; I don't have to talk to someone if I don't want to.
- I will remember not everyone is who they say they are on the Internet. I have a right to tell someone I trust if I think anyone is suspicious.
- I have the right to not be videoed or photographed by anyone using cameras, webcams or mobile phones without my permission and for those to not be shared without my permission.
- I have a right not to be bullied or intimidated by others through technology (including my phone and social media accounts) and I have the right to report this if this happens.
- I have the right to not be judged by others when I report something that makes me feel uncomfortable or violates my privacy.
- If I accidentally see something I shouldn't, I have the right to tell someone and not to feel guilty or judged about it.
- We are all responsible for treating everyone online with respect. You should not use behaviour or language that would be offensive or upsetting to somebody else.

User's Digital Responsibilities

Students are responsible for good behaviour on the Internet just as they are in a classroom or a College corridor. General College rules apply, it is presumed that users will comply with College standards and will honour the agreements they have signed.

The following digital responsibilities are not exhaustive but provide a guide to the expected standards in the college.

Web Access	Internet usage should be purposeful and directed to specific goals relevant to your learning.
E-Mail and Social Media	All users are expected to communicate with the same appropriate, safe, mindful, courteous conduct online as offline. All staff and students have an individual email account. All network users must use their school email account for all college related correspondence. Cyberbullying will not be tolerated. This includes (but is not limited to): obscene language, harassing, dissing, flaming, denigrating, impersonating, outing, tricking, excluding and cyberstalking.
College-Owned Devices	All users are expected to treat these devices with extreme care and caution. Users should report any loss, damage or malfunction of College-owned devices to the IT Department.

Personally- Owned Devices	Users are expected to ensure that personally owned devices are secure and free of viruses and malicious applications and compliant with the college's BYOD policy. The IT Department may provide a limited amount of support to users but any loss or damage are ultimately the responsibility of the owner.
Downloads and Streaming	Users should not download, attempt to download or run executable programs on the College network without express permission from the IT Department. Download or streaming of any media files (e.g. video or audio) should be for education purposes, and in line with the terms of their license agreement.
Netiquette	All users should recognise that among the valuable content online there is also unverified, incorrect or inappropriate content. Users should only use trusted sources when conducting research via the Internet.
Copyright and Plagiarism	Users should cite or give credit to the original author of information or media (images, audio and video) contained in their work. If possible you should seek permission from the original author.
Personal Safety	Users should never share personal information (including home address, phone number, date of birth, financial information) or media (images, audio and video) that could be used to identify me, my family or my friends, unless a trusted adult has given permission. Users should report any incident that makes you concerned for your personal safety immediately. It is recommended that you save or take screenshots to help any further investigation.
Data Protection	Users should exercise caution if there is a need to transfer personal data stored on the College network to other devices (including memory sticks, cloud storage and personal computers/phones/tablets). In these instances, you should follow the guidance provided by the College's Data Protection Policy.
Remote education provision	User should ensure to use a safe and appropriate place to access remote learning if college/setting is closed in response to Covid-19 or they have to self-isolate. Users will ensure their access to remote learning is appropriate using college online systems. When accessing video learning, they will ensure to use am an appropriate location and dress suitably.

Security

System accounts are to be used only by the authorised owner of the account. Users may not share their account or password with another person or leave an open file or session unattended or unsupervised.

Users are expected to take reasonable safeguards against the transmission of security threats over the College network. This includes not opening or distributing infected files or programs and not opening files or programs of unknown or untrusted origin.

If you believe a computer, mobile device or an external storage device you are using might be infected with a virus please alert a member of the IT Department. Do not attempt to remove the virus yourself or download any programs to help remove the virus.

Violations of this Acceptable Use Policy

Any access to Information and Communications Technology (ICT) facilities and resources within Brampton College are subject to the compliance of the guidelines as set out in this policy and any other policy relating to the use of ICT equipment.

Computer access within the College requires responsibility. Any breach of the regulations stated in this policy might have the following consequences:

- Temporary or permanent ban of a user account;

- Temporary or permanent ban of a user's personal device;
- Additional disciplinary action may be added in line with existing practice on inappropriate language or behaviour;
- When applicable, police or local authorities may be involved.

Online safety

If you are worried about the way someone is communicating with you online, the following sources can prove useful to protect you.

Child Exploitation and Online Protection command
https://www.ceop.police.uk/Safety-Centre/

Childline (Online and on the phone anytime)
https://www.childline.org.uk/
Phone: 08001111

Thinkuknow
https://www.thinkuknow.co.uk/

Other notes

The use of College IT systems and resources are subject to the following statutes and regulations:

The Copyright, Designs and Patents Act 1988
Computer, Copyright Software Amendment Act 1985
The Computer Misuse Act 1990
UK General Data Protection Regulation (UK GDPR)
The Electronic Communications Act 2000
The Freedom of Information Act 2002
The Regulation of Investigatory Powers Act 2000
Trade Marks Act 1994
Criminal Justice and Public Order Act 1994
Copies of these documents are available online at http://www.opsi.gov.uk/