e-Safety and IT Acceptable Usage policy

Purpose & Scope

West Thames College recognises that the internet and other digital learning technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and students learn from each other. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Students with internet access are more confident and have been shown to produce better-researched, more effective and well-presented work. We encourage the use of technology in order to enhance skills and promote achievement. However, the accessible and global nature of the internet and variety of technologies available mean that we are also aware of potential risks and challenges associated with such use. Our approach is to implement e-Safety within the college and to support staff and learners to identify and be aware of these risks. We believe this can be achieved through a combination of security measures, training and guidance and implementation of our associated policies. In furtherance of our duty to safeguard learners and the "Every Child Matters" agenda, we will do all that we can to make our learners and staff stay e-Safe and to satisfy our wider duty of care.

This policy stipulates the practices and constraints that apply when accessing and using the college's internet enabled resources and platforms to ensure the use of technology and platforms are used in a safe and controlled manner by staff, students and other authorised visitors.

This policy applies to:

- Students, staff, visitors or contractors who access the college IT services on college provided equipment/services and anyone using their personal devices via BYOD (Bring Your Own Device)
- All forms of IT services administered or supported by the college such as back office systems and other third party externally hosted services provided by the college e.g. Moodle (VLE), Office 365 (this includes Emails & Teams)
- The use of the college's hardware, software, network storage, data and resources.
- All information held by the college regardless of the format in which it is held

This policy provides overarching direction for IT services and e-resources across the College and incorporates the JANET Acceptable Use Policy and the JANET Security Policy published by JANET (UK), the Combined Higher Education Software Team (CHEST) User Obligations, together with its associated Copyright Acknowledgement. There may be other related policies and specific subsidiary procedures covering a range of IT user activities and aligned with this policy that must also be followed also.

All existing users of ICT will be notified of this policy and future changes via various channels such as during college PC Logon information, Wifi logon, Moodle, Staff intranet etc.

e-Safety

The use of technology has become a significant component of many safeguarding issues. Child sexual exploitation; radicalisation; sexual predation: technology often provides the platform that facilitates harm. An effective approach to online safety empowers a school or college to protect and educate the whole school or college community in their use of technology and establishes mechanisms to identify, intervene in, and escalate any incident where appropriate.

The breadth of issues classified within online safety is considerable, but can be categorised into three areas of risk:

Content

- Exposure to age-inappropriate material
- Exposure to inaccurate or misleading information
- Exposure to socially unacceptable material, such as that inciting violence, hate, extremism or intolerance
- Exposure to illegal material, such as images of child abuse
- Illegal Downloading of copyrighted materials e.g. music and films

Contact

- Grooming using communication technologies, potentially leading to sexual assault or child
- Radicalisation the process by which a person comes to support terrorism and extremist ideologies associated with terrorist groups.
- Cyber-bullying via websites, mobile phones or other forms of communication device

C**onduct**:

- personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images, or online bullying.

The Prevent duty (Counter-Terrorism and Security Act 2015)

This statutory guidance makes clear the need for Colleges to ensure that Staff and Students are safe from being drawn into radicalisation, terrorist and extremist material when using any devices or platforms provided by the college to access the internet

Online communication between students and staff should only be done through the college provided resources such as Moodle (VLE) or Office 365 (using email or Teams) or other as deemed appropriate. Staff must never use their personal mobile, email, social media or other platforms to initiate and communicate with students.

The users continued use of resources and platforms will constitute acceptance and agreement to this policy

Unacceptable usage of provided resources: -

The following are examples of unacceptable use, the list is not exhaustive: -

- Creating, transmitting, storing or displaying insulting, indecent or obscene material.
- Creating, transmitting, or displaying material that deliberately and unlawfully discriminates, or encourages deliberate and unlawful discrimination, on the grounds of race, ethnicity, gender, sexual orientation, marital status, age, and disability, political or religious beliefs.
- Creating, transmitting or displaying defamatory material.
- Obtaining, transmitting or storing material where this would breach the intellectual property rights of another party. This includes downloading and sharing music, video and image files without proper authority.
- Contravening the policy of a third-party company with which the college holds a contract for IT services.
- Creating or transmitting material with the intent to defraud.
- Creating or transmitting material or using college systems for commercial purposes unrelated to the interests of the college.
- Causing annoyance or inconvenience, e.g. sending unsolicited email chain letters, unauthorised bulk email (spam), which is unrelated to the legitimate business of the college.
- Sharing information when not authorised to do so (especially commercially sensitive, personal and sensitive personal data).
- upload or download pirated software, music or videos
- disclose to a third party the personal details of any other member of the College community, without their consent
- Intentionally interfering with the normal operation of the network, including the spreading of computer viruses, malware, ransomware (or similar) and sustained high volume network traffic that substantially hinders others in their use of the network.
- Access to the “Dark Web“ or Tor Networks

- Users must not attempt to set-up or use any by-pass software, in order to bypass any College Internet /Email filtering or other security measures.
- Deliberate activities having, with reasonable likelihood, any of the following characteristics:
  - Wasting staff effort or time unnecessarily on IT management.
  - Corrupting or destroying other users' data.
  - Violating the privacy of other users.
  - Disrupting the work of other users.
  - Denying service to other users (for example, by deliberate or reckless overloading of access links or switching equipment).
  - Continuing to use an item of networking software or hardware after a request that use should cease because it is causing disruption to the correct functioning of the network.
  - Other misuse of network resources, such as the introduction of computer viruses, malware, ransomware or other harmful software.
  - Any breach of industry good practice that is likely to damage the reputation of the JANET network will also be regarded as unacceptable use of the College Network.
  - Introduce data-interception, password-detecting or similar software or devices to the College's Network.

Username, Password and Authentication Measures

- You must take all reasonable precautions to safeguard your username, password and any other IT credentials issued to you.
- You must not allow anyone else to use your IT credentials.
- No-one has the authority to ask you for your password, and you must not disclose it to anyone, including the IT Service Desk.
- You must not attempt to obtain or use anyone else's credentials, and you will be held responsible for all activities undertaken using your IT credentials. You should only use the access to College systems provided to for the purpose which that access was granted.
- You must not impersonate someone else or otherwise disguise your identity when using the IT facilities.
- Passwords must be unique to the system being accessed and not used to access any other system.
- Passwords must be changed every 60 days.
- Passwords may be changed at any time. Please contact the IT Helpdesk for further assistance or advice on passwords.
- Users take full responsibility for any activity which takes place while logged in using their User Account
- In order to access some IT services, the college may require users to authenticate their identity through secondary measures such as Multi-Factor Authentication (MFA) technology. To access those systems where MFA technology has been enabled, users will be required to provide unique information sent to them via an independent method such as an authenticator software application, SMS message to a pre-registered mobile device or a similar alternative method supported by the college, in addition to their username and password.

Confidentiality

- Individuals who handle personal, confidential or sensitive information must take all reasonable steps to safeguard it and must be aware of and observe the requirements of the college obligation under Data Protection and GDPR legislation
- Any breaches of confidence relating to confidential information held by the college may be treated as a disciplinary offence (under either staff or student disciplinary procedures) and may constitute an offence under data protection legislation or regulation.
- Users must ensure that any data exported from university systems is handled in such a way as to maintain the confidentiality and security of that data.

E-mail

This policy covers the use of college email accounts assigned to individuals or groups. It also applies to other collaborative tools and shared mailboxes where these tools make use of the college's email service

- The College's email system is a core business application, it should not be used for political, business or commercial purposes unrelated to the business of West Thames College.

- Email users must take reasonable measures to prevent the transmission of viruses, such as not opening email attachments received from unsolicited sources
- The provisions of the Data Protection Act 1998 (and any related legislation such as GDPR) the Freedom of Information Act 2000 and the college policies and procedures relating to Data Protection, Freedom of Information and Confidentiality also apply to email communication. This means that emails may have to be disclosed to individuals or outside agencies, as required by current Data Protection and Freedom of Information legislation or as required by any other statutory or legal duty imposed on the college
- Email users must always use the college approved encryption methods when sending personal or sensitive information outside the college network.
- All users are expected to check their e-mail mailbox on a regular basis.

SPAM & Phishing Emails

SPAM email is unsolicited email, often referred to as 'junk' email and is indiscriminately sent to many thousands (if not hundreds of thousands) of email addresses. SPAM email usually invites you to purchase a product or service.

Be aware of emails which may impersonate another college email and attempt to re-direct you to an external link for an attempt to carry out a Phishing attack. If in doubt, always confirm the email validity with the person directly by phone.

Incident Reporting

Any security breaches or attempts and any unauthorized use or suspected misuse of ICT must be immediately reported to IT Services or a member of the Executive Team (ET). Additionally, all security breaches, lost/stolen equipment or data, virus notifications, unsolicited emails, misuse or unauthorized use of ICT and all other policy non-compliance must be reported to IT Services.

Helpdesk & ICT Support Services

ICT services and support are provided through the IT Service Desk on 020 8326 2326 (ext. 2326) or can be found in Spring Grove House (Room SB07)
In order that requests can be dealt with efficiently, staff must report all requests or incidents to the IT Services Team.

Appendix

Useful Links for Further Information:

- Child Exploitation & Online Protection Centre http://www.ceop.police.uk
- Keeping children safe in education 2021 - https://assets.publishing.service.gov.uk
- Internet Watch Foundation https://www.iwf.org.uk/
- NIDirect-'Staying Safe Online' https://www.nidirect.gov.uk/articles/staying-safe-online-0
- Get Safe Online http://www.getsafeonline.org
- *JANET User Acceptance policy - https://community.jisc.ac.uk/library/acceptable-use-policy*

Related Legislation:

- Computer Misuse Act 1990
- Data Protection Act 1998
- Copyright, Designs & Patents Act (1988)
- Computer Misuse Act (1990)
- Criminal Justice & Public Order Act (1994)
- General Data Protection Regulation (2018)
- Human Rights Act (1998)
- Regulation of Investigatory Powers Act (2000)
- Lawful Business Practice Regulations (2000)
- Communications Act (2003)
- Counter terrorism and Security Act (2015)
- Police & Justice Act (2006)

Opportunities to teach safeguarding, including online safety:

- Be Internet Legends developed by Parent Zone and Google is a free internet
- safety curriculum with PSHE accredited lesson plans and teaching resources for Key Stage 2 pupils
- Disrespectnobody is Home Office advice and includes resources on healthy relationships, including sexting and pornography
- Education for a connected world framework from the UK Council for Internet Safety supports the development of the curriculum and is of particular relevance to RSHE education and Computing. It is designed, however, to be usable across the curriculum and beyond (covering early years through to age 18) and to be central to a whole school or college approach to safeguarding and online safety.
- PSHE association provides guidance to schools on developing their PSHE curriculum
- Teaching online safety in school is departmental guidance outlining how schools can ensure their pupils understand how to stay safe and behave online as part of existing curriculum requirements
- Thinkuknow is the National Crime Agency/CEOPs education programme with age
- specific resources
- UK Safer Internet Centre developed guidance and resources that can help with the teaching of the online safety component of the Computing Curriculum.