ICT Acceptable Use Policy for Students

2020/21

Signature:

Head teacher

Approval Date:
Review Date: September 2021
ICT Acceptable Use Policy for Students

Aims

The aims of this Acceptable Use Policy are:

- To ensure that students may benefit from the learning opportunities offered by the college’s network and internet resources in a safe and effective manner
- To protect the college’s ICT infrastructure from misuse and attack

The College Undertakes to:

- Prioritise Data Protection and adhere to strict guidelines on the use of personal or sensitive information
- Provide a safe and productive digital learning environment
- Provide students with training in the area of internet safety
- Supervise students’ network and internet access wherever possible
- Monitor students’ network and internet activities using software systems
- Provide internet filtering in order to minimise the risk to inappropriate material
- Ensure there is a secure and regular backup of student data wherever possible. Nevertheless, students are still primarily responsible for backing up their own data and work
- Ensure that robust and up to date virus detection and security systems are in place to protect students’ data
- Only publish students’ projects, artwork or college work on the college website/internet in line with agreed college policy

Important Information for All Students:

- Use of ICT Facilities is forbidden unless supervised by a member of staff
- Network and Internet use and access is considered a college resource and a privilege
- If the college Acceptable Use Policy is not adhered to, this privilege will be withdrawn and appropriate sanctions will be imposed
- Designated staff can review student files and communications to ensure that the system is being used responsibly. They also have the right to access computer storage areas, accounts and removable media, including USB Flash Drives and CD-ROMs
- Designated members of staff can remotely view a student’s computer screen at any time, without them knowing, in order to ensure compliance and appropriate use of the West Somerset College network
- Students are subject to the provisions of the Copyright, Designs and Patents Act 1988
- The college will provide information on the following legislation relating to use of the West Somerset College network, which teachers, students and parents/carers should familiarise themselves with: The Data Protection Act 1998; Data Protection (Amendment) Act 2003; Video Recordings Act 1989; Copyright, Designs and Patents Act 1988; and Computer Misuse Act 1990

Students will:

- Ask a teacher before using any personal USB flash drive, CD-ROM or similar device in college
- Observe good etiquette at all times and behave in a way that reflects well on them and the college
• Use the West Somerset College network for college related matters only, use computers for educational purposes and adhere to the student print policy
• Make sure they take regular backups of their work
• Respect other computer users and never harass, harm, cause insult or offence
• Respect the security protocols in place on the computers and not attempt to bypass or alter security settings put in place on the West Somerset College network. Attempting to bypass or breach the college security systems is a serious offence
• Use approved college email accounts for college use only. Personal email accounts such as hotmail and gmail are prohibited
• Only use discussion forums or other electronic communications that have been approved by the college
• Report any damaged ICT equipment (accidentally or otherwise) to the supervising member of staff immediately
• Read and adhere to college information on e-Safety, cyber-bullying and social networking guidance

Students will NOT:

• Attempt to upload, download or transfer any software from the internet or portable media
• Attempt to bypass the college’s internet filters. Violation of this is a serious offence
• Copy software or multimedia content unless it has been approved by a member of staff
• Install, attempt to install, or store programs of any type on the West Somerset College network
• Use the internet, computer systems, portable media or other mobile devices for playing non-educational games
• Store personal photographs, music, games or other prohibited/inappropriate content in their user area (R: Drive) or anywhere on the college network
• Damage, disable, dismantle or otherwise cause, or attempt to cause harm to the operation of computers, or any other ICT equipment or cables
• Attempt to connect mobile equipment (eg laptops, tablets, PSPs, mobile phones etc) to the college network
• Eat or drink in any room where there is ICT equipment
• Reveal their password to anyone, or use someone else’s username or password. Students are responsible for the actions of anyone who is using their username and password, so must immediately tell a member of staff if they suspect that someone else has this information
• Access or alter other people’s folders, work or files without permission
• Visit Internet sites that contain obscene, illegal, hateful or otherwise objectionable materials, including any website containing any form of extremist propaganda or promotion of radicalisation. Any such sites should be reported to a member of staff immediately
• Send or receive any material that is illegal, obscene, defamatory or intended to annoy or intimidate another person
• Use social networking sites, such as Twitter or Facebook while in college, or use such platforms to make public comments about West Somerset College, its staff or students, which are defamatory, liable to cause offense or bring the college into disrepute
• Pass personal information on (like real names or addresses) to anyone on the internet