Reference Number: *P32*

YEOVIL COLLEGE STUDENT IT ACCEPTABLE USE POLICY

PURPOSE OF THE POLICY

Yeovil College encourages all students to use ICT, the internet and a wide range of technology to support them and develop independent learning skills. However, it is essential that all students ensure safe, appropriate and responsible use of such technologies.

SCOPE

This policy applies to any activity undertaken both on College premises and off College premises and links with the e-safety protocol.

RESPONSIBILITY AND AUTHORITY

Students will:

- Only access the College IT system using "my user" account and password which they will not share with anyone else.
- Make sure the language they use in all electronic communication is appropriate and suitable, including mobile phones, social networking sites, emails and VLE forums.
- Respect copyright of all materials and will avoid plagiarism (copying of someone else's work including from the internet) when using IT to produce their work.
- Only use College IT facilities for coursework and study purposes to support their learning.
- Access social networking outside of session time.
- Inform a member of staff immediately if they inadvertently access unsuitable material.

Students will not:

- Use any device that is logged on by another user.
- Deliberately interfere with and/or delete another person's files.
- Use social media during teaching and learning sessions unless directed as part of teaching.
- Send, create or publish anything which others might reasonably find offensive, including use of inappropriate imagery on mobile devices.
- Use mobile phones, cameras or other electronic devices to take, publish or circulate pictures or videos of anyone without their permission.
- Access, share or receive unsuitable material that is pornographic, racist, discriminatory or extremist. This includes material containing physical violence or could cause mental harm. Offensive material or those promoting illegal substance misuse are also prohibited.
- Use College systems for harassment or bullying of another learner or member of staff
- Deliberately cause damage to network or other electronic equipment by means of harmful files or programs (eg virus infections, malware, hacking or physical tampering or stealing of equipment).
- Deliberately try to bypass filters or other safeguards employed by the College.
- Use College systems to run a private business.
- Attempt to install or download any additional software onto College systems.
- Store personal photographs, music or video downloads on the College network.

Students must understand:

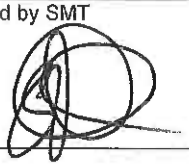
- They are wholly responsible for their account and if they do share their details they will be held responsible for any activity carried out on that user account, which could result in disciplinary action or contacting the Police or Channel.
- That logs are kept of all software usage, websites visited from College systems and personal devices and emails sent from College and wireless systems.
- IT services may check their personal documents for viruses and unsuitable material at any time if there is reason for concern or links to safeguarding and Prevent.

Failure to comply will lead to the following consequences:

a. Their account will be blocked pending investigation and it may result in the account being locked for a period of time.
b. Disciplinary process will be started.
c. Persistent or serious offenders will be suspended pending further investigation and Police and Channel may be involved.
d. A permanent block may be applied.
e. All students must read and understood the above statements and agree to comply with Yeovil College rules for use of IT services in conjunction with the e-safety protocol.

RELATED POLICIES, PROCEDURES, DOCUMENTS, DEFINITIONS

Student Disciplinary Procedure
Student Code of Conduct
Safeguarding Policy and Procedure

Policy Review				
Author	Position	Approved by SMT	Approval date	Review date
Craig Cullen & Michelle Dennett	Head of Estates & IT Services and Head of Student Experience	Signed: 	27.09.17	September 2019

Document Control – Revision History (Policies only)

Author/Owner	Summary of Changes	Date	Date last reviewed by SED	Recommend to SED Y/N
Craig Cullen/ Michelle Dennett	Minor amendments to clarify points.	13.09.17	09.09.15	No

Initial Equality Impact Screening

Have you consulted on this policy?
Details: Yes, with Director of Teaching & Learning and Quality, Prevent Board.

What evidence has been used for this assessment? Equality Duty, Prevent Duty, Safeguarding Policy

Could a particular group be affected differently in either a negative or positive way? Indicate Y where applicable. No

Group	Negative impact	Positive impact	Evidence
Age			
Disability			
Gender (incl. Transgender)			
Race (incl. Gypsy &Traveller)			
Religion or belief			
Sex			
Sexual orientation			
Marriage & civil partnership			
Pregnancy & maternity			
Other groups (see guidance)			

Please give details:

If any negative impacts are identified, are there any related polices, services, strategies, procedures or functions that need to be assessed alongside this screening? If yes, please detail below:

Should the policy proceed to a full Equality Impact Assessment? No
If no, please give reasons: it is an additional document to support E-Safety Protocol.

Declaration
We are satisfied that an initial screening has been carried out on this policy and a full Equality Impact Assessment is not required.

We understand that the Equality Impact Assessment is required by the College and that we take responsibility for the completion and quality of this assessment

Completed by Author: Craig Cullen/Michelle Dennett Position: Head of IT Services/Head of Student Experience
Date: 03.08.15

Reviewed by Safeguarding, Equality & Diversity Group: Date: 09.09.15

Comments from Safeguarding, Equality & Diversity Group Review: