Reference Number: *P29*

SOFTWARE LICENSING & MANAGEMENT POLICY

Policy Review					
Author	Position	Approved by SLT	Approval date	Review cycle:	Published Y/N
Gareth Bevan	IT Services Manager	Signed: 	28.04.26	2 Years April 2028	Y

Author	Summary of Changes	Date	Version	Recommend to SED Y/N
Craig Cullen	Minor amendments	11.05.16		Y
Craig Cullen	Minor amendments	24.05.18		N
Craig Cullen	Minor amendments	14/09/22	v1	
Shane Tighe	Privacy Impact Assessment (PIA) information added	15/3/23	v1.1	
Gareth Bevan	Substantial amendments to draw focus to cloud services and inclusion of software & systems services compliance procedure.	14/10/25	V2	

Initial Equality Impact Screening

Has anyone else been consulted on this policy and/or procedure? Craig Cullen, Karen Foster, Katie Lister

What evidence has been used for this impact screening (e.g. related policies, publications)?
Acceptable use of It policy

Declaration (please tick one statement and indicate any negative impacts)

[X] I am satisfied that an initial screening has been carried out on this Policy and/or Procedure and a full Equality Impact Assessment is not required. There are no specific negative impacts on any of the Protected Characteristics groups.

[ ] I recommend that an Equality Impact Assessment is required by the Equality and Diversity group, as possible negative impacts have been identified for one or more of the Protected Characteristics groups as follows:

- ☐ Age
- ☐ Disability
- ☐ Gender Reassignment
- ☐ Race
- ☐ Religion or belief
- ☐ Sex
- ☐ Sexual orientation
- ☐ Marriage & civil partnership
- ☐ Pregnancy & maternity

Completed by:	Gareth Bevan	Position:	IT Services Manager	Date:	15/11/25

☐ Reviewed by Equality & Diversity Group: NO If Yes: Date:

☐ I confirm that any recommended amendments have been made

Summary of Comments/Recommendations from Equality & Diversity Group Review:

Amended by Author:		Position:		Date:	

Contents

1. PURPOSE OF THE POLICY

The purpose of the Software Licensing & Management Policy is to ensure that the College:

1.1 Legal compliance & risk mitigation

To ensure the College only uses legally licensed software, avoiding copyright infringement, cyber security risk, potential lawsuits, and significant financial penalties that can result from using insecure, unlicensed or pirated software.

1.2 Financial control

To help the College track software purchases, avoid redundant licensing costs, negotiate better volume discounts, and prevent unauthorized spending on software that may already be available across the college.

1.3 Security and stability

To ensure that only approved, vetted applications are accessed from college systems, reducing vulnerabilities, malware risks, and compatibility issues that could disrupt operations or compromise sensitive college and student data.

1.4 Resource optimisation

To enable the IT Services department to standardise software across all college departments, making it easier to provide technical support, train staff, and maintain systems efficiently. To avoid the duplication of resources and data across software and web-based platforms. It also helps identify underutilised licenses that could be reallocated to other areas.

1.4 Accountability and governance

To establish clear guidelines for departments, staff, and students about what software they can use, who approves purchases, and what responsibilities system owners have over their department software use, creating a framework for responsible technology use across the College.

2. SCOPE

2.1 This policy applies to all College staff/learners and pertains to both educational and administrative software.

2.2 Software is defined as any application that requires installing on to our college IT systems, or any external web based system that requires college information on our staff or students (even where anonymised)

2.3 The College is committed to installing and using only College approved, licenced and legally procured software. The College will not condone the use of unapproved or unlicensed software. Where unlicensed software is found by IT Services, it will be removed, and staff or students found to be installing unlicensed software will be liable to disciplinary action.

2.4 The College recognises that staff and students engage with digital tools in a wide variety of roles and contexts. This policy is designed to support safe, compliant and effective use of software, and to provide clear guidance and support where new tools or systems are required.

2.5 Further, in order to maintain a level of software which it is affordable to upgrade appropriately and in a timely fashion, only fully authorised software may be used on College networks and computers.

2.5.1 The decision to introduce new critical software or to upgrade major core software from one generation to the next is dependent on the compatibility and compliance of cyber security standards defined within Cyber Essentials and if applicable, the Department for Education's "Cloud solution standards for schools and colleges".

2.5.2 New critical system software or upgrading major core software from one generation to the next must be included in individual Department Business Plans (in line with the ITS Strategy and IT Disaster Recovery Plan). It must meet College Financial Regulations and be subject to budget approval in the IT Software budget. Requests for new software and services must align with

annual budget setting processes, where budget has not been allocated – the first year of a product or service must be paid for from the department requesting the software or service. Finally, all requests must be approved by the ECO group and final approval by the Senior Leadership Team. System owners are expected to work in partnership with IT Services and Finance to ensure that all required approvals, compliance checks and planning activities are completed before any financial commitments or upgrades are agreed with external parties.

2.5.3 IT Services maintains a list of approved software and cloud-based platforms. Any request for software not currently on the approved list, must follow the 'Software and System Services Compliance Process'. The first step in the process is to access the Software & System Services Compliance Documentation, under the IT Services section in staff forms library. Here you will find access to the full guidance documentation, questions sets and the Software Investigation Agent to support your initial findings. Upon completion, approval will be required from ECO group for vetting and a full system compatibility and compliance test.

There will be a Technical Consultation Process that will ensure compliance checks are made to review cyber security, geographical access requirements, GDPR, safeguarding, web accessibility and AI capability. A College technical team will review compatibility and integration to ensure accuracy and effective use of existing college data and systems. This report will then need to be provided to ECO group for final sign off prior to purchase agreement.

2.5.4 In exceptional circumstances, if after compliance testing, the software is approved by ITS and is not within budget, the approval of purchase will go to SLT with a business case to be agreed pending affordability and judgement of need.

2.5.5 The IT Services Manager will ensure the overall licensing arrangements for approved College software are maintained.

The IT Services Manager is responsible for the licensing and maintenance of:

- Server & Client Operating Systems
- System security applications
- Office products and layered software
- Web based applications such as exam software
- Database server & client Licensing
- Core College Applications, as used in Administration (and including licensing of Academic use of those Core Applications)

2.5.6 All local software installations to the College networks must be undertaken by IT Services, or, where appropriate, MIS and must adhere to the best practice and administrator access restrictions as set out in the Acceptable Use of IT policy.

2.5.7 All cloud-based software and Software as a Service (SaaS) where data is inputted or exchanged will require an initial scoping discussion which will recommend that a Data Privacy Impact Assessment (DPIA) is carried out, and the Data Protection Officer (DPO) will review the need for a Data Sharing Agreement or a contractual GDPR arrangement; as stipulated in the GDPR Policy After initial scoping is successful, the staff member would be requested to begin the DPIA process. The requesting staff member must email data.protection@yeovil.ac.uk to begin the DPIA process.

2.5.8 All cloud-based software or Software as a Service (SaaS) solutions will have a nominated system owner. System owners are responsible for overseeing compliance and governance requirements, with guidance and support provided by IT Services and relevant College teams. These requirements are set out by the NCSC's Cyber Essentials and the Department for Education's "Cloud solution standards for schools and colleges" - both of these related materials can be found under the References section within this policy. To assist these system owners in achieving their responsibilities there is a Software and Systems Services Compliance Procedure that must be followed when introducing any additional or substantial changes to cloud systems or software.

3. RESPONSIBILITY AND AUTHORITY

The overall responsibility for the Policy lies with the Head of Infrastructure. The implementation of its purchasing provision is overseen by the VP Finance & Corporate Services. Software licencing is the responsibility of the IT Services Manager.

4. RELATED POLICIES, PROCEDURES, DOCUMENTS, DEFINITIONS

4.1 References

Associated documents are:

- Acceptable Use of IT Policy
- The College Digital Strategy
- IT Services Request for Software Process
- Data Protection Policy
- Safeguarding Policy
- Web Accessibility Regulations 2018
- Software and Systems Compliance Procedure
- Data Protection Officer Procedures – Appendix G "DPIA Process"
- NCSC Cyber Essentials - Link
- Cloud solution standards for schools and colleges – Department for Education Link

4.2 Definitions

'Software' within this Policy means all programs, applications, routines etc present either on the College network or stored on College stand-alone computers. The definition is not restricted to large-scale commercial application software.

'Unlicensed Software' refers to software that is not legally obtained or being used in accordance with the software vendors terms of service. Potentially placing financial risk on the business through its unapproved use.

‘Cloud-based software’ refers to applications or services that are hosted on remote servers and accessed over the internet, rather than being installed and run on a local computer or server on campus.

‘Software as a Service (SaaS)’ is a way of delivering a software platform over the internet. The software is hosted by a provider and is typically offered on a subscription basis. The college is responsible for configuring and maintaining the service.