Policy/Procedure Title	e-Safety Policy
Review Cycle (**Please specify*)	Yearly
Responsible Department	IT Services
Procedure *Owner (**Overall responsibility*)	Head of IT Services
Responsible *Person (*if different to above*) *responsibility for communicating changes and staff training where appropriate	
Types of provision this procedure applies to: (*delete as appropriate*)	All staff and learners

Revision Record		
Rev. No.	**Date of Issue**	**Details and purpose of Revision:**
1	24/07/2023	Dates of regs and acts updated
2	14/08/2024	Description of GDPR added
3	10/06/2025	Reviewed
4	12/02/2026	Reviewed

Equality Impact Assessment

Whenever a policy is reviewed or changed, its impact assessment also must be updated. The Equality Act 2010 seeks to simplify discrimination law and introduced statutory duties to promote equality whereby The College of West Anglia must, in the exercise of its functions, pay due regard to the need to promote equality in relation to the protected characteristics.

Could any staff or students be adversely impacted by this policy/process? If yes give details and how this will be mitigated:

Date:	**Action and Monitoring:**

E, D & I Statement

This procedure has been reviewed in line with the Equality Act 2010 which recognises the following categories of individual as Protected Characteristics: Age, Gender Reassignment., Marriage and Civil Partnership, Pregnancy and Maternity, Race, Religion and Belief, Sex (gender), Sexual Orientation and Disability. We will continue to monitor this procedure to ensure that it allows equal access and does not discriminate against any individual or group of people.

Contents

Introduction

The College of West Anglia recognises the benefits and opportunities which technologies offer to teaching and learning. Our approach is to implement safeguards within the college and to support staff and learners to identify and manage 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, including meeting the Keeping Children Safe in Education (KCSIE) requirements, 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 e-safety policy should be read in conjunction with other relevant college policies and procedures.

The policy applies to all users who have access to the college IT systems, both on the premises and remotely, and to all use of the internet and electronic communication devices such as email, mobile phones, games consoles, social networking sites, etc.

Objectives

1. Safeguards on college IT-based systems are strong and reliable.
2. Behaviour of users of systems is safe and appropriate.
3. Storage and use of images and personal information on College IT- based systems is secure and meets all legal requirements.
4. Staff and students are well educated in e-safety.
5. Any incidents which threaten e-safety are professionally managed.
6. Students understand the risks attached to accessing terrorist and extremist material online and understand the institution's duty and process in these areas.

Intended Outcomes

1. Security

1.1 College networks are safe and secure as far as possible, with appropriate and up-to-date security measures and software in place.

1.2 Digital communications, including email and internet postings, over the college network, are monitored as far as is practicable.

2. Behaviour

2.1 All users of technology adhere to the standards of behaviour set out in the Code of Conduct, Student Code of Behaviour, and the IT Acceptable Usage Policies signed at induction.

2.2 All users of IT adhere to college guidelines when on email, mobile phones, social networking sites, games consoles, chat rooms, video conferencing and web cameras, etc.

2.3 Any abuse of IT systems and any issues of bullying or harassment (cyber bullying) online are dealt with seriously, in line with staff and student disciplinary procedures.

2.4 Any conduct considered illegal or extreme is reported to the police or appropriate authorities.

3. Use of images and video

3.1 The use of images or photographs is encouraged in teaching and learning.

3.2 There must be no breach of copyright or other rights of another person.

3.3 Staff and students are trained in the risks of downloading, posting, and sharing images, and particularly of the risks involved in posting personal images onto social networking sites, for example.

3.4 College staff provide information to learners on the appropriate use of images, and on how to keep their personal information safe.

3.5 Advice and approval from a senior manager is sought in specified circumstances or if there is any doubt about the publication of any image.

3.6 Published photographs do not include names of individuals without clear consent.

4. Personal information

4.1 Processing of personal information is done in compliance with The Data Protection Act 2018 and The General Data Protection Regulation (GDPR) 2018.

4.2 Personal information is kept safe and secure and is not passed on to anyone else without the express permission of the individual.

4.3 Staff always keep learners' personal information safe and secure.

4.4 Every user of IT facilities logs off on completion of any activity or locks the machine or ensures rooms are locked if unsupervised, where they are physically absent from a device or when accessing web-based services remotely.

4.5 Personal data no longer required, is securely deleted.

5. Education and Training

5.1 Staff and learners are supported through training and education to develop the skills to be able to identify risks independently and manage them effectively.

5.2 Learner induction and the programme of pastoral tutorials contain sessions on e-safety and the need for students and staff to be aware of the consequences of inappropriate use of IT systems and specific websites.

5.3 Learners are guided in e-safety across the curriculum and opportunities are taken to reinforce e-safety messages.

5.4 Learners know what to do and who to talk to where they have concerns about inappropriate content.

5.5 In classes, learners are encouraged to question the validity and reliability of materials researched, viewed, or downloaded. They are encouraged to respect the copyright of other parties and to cite references properly.

5.6 Staff are e-safety trained. Further resources of useful guidance and information are issued to all staff as available.

6. Incidents and response

6.1 A clear and effective incident reporting procedure is maintained and communicated to students and staff.

6.2 Reports of e-safety incidents are acted upon immediately to prevent, as far as reasonably possible, any harm or further harm occurring.

6.3 Action following the report of an incident might include disciplinary action, sanctions, reports to external agencies (e.g. the police), review of internal procedures and safeguards, pastoral support for affected students, etc.

7.4 Any breaches of this policy should be reported in the first instance to the Assistant Principal Student Services.

Responsibilities

The **Assistant Principal Funding and Performance** is responsible for maintaining this policy and for maintaining best practice in IT procedures and practices to manage any e-safety risks effectively.

The **Assistant Principal Student Services** is responsible for investigating reported breaches and for all e-safety matters in relation to college staff.

The **Student Advisers and Counsellor** for providing pastoral and practical support for students dealing with issues related to e-safety.

The **Vice Principal Curriculum and Quality** for incorporating e-safety in student induction and the pastoral tutorial framework.

Tutors for delivering an appropriate programme of education. and for embedding e-safety education and practice into their teaching programme.

All College Managers for implementing good e-safety practice and safeguards consistent with this policy in their area of responsibility.

The College Safeguarding Board for overseeing and reviewing e-safety arrangements.

All members of college staff and volunteers for staying alert to and responding appropriately to any potential or actual e-safety issue.