E-Safety Policy 2026-2027

Effective for employees, students, governors and volunteers September 2026

Overall responsibility:	Principal
Implementation:	ICT Manager/Assistant Principal Student Services
Date issued:	September 2026
Date for review:	September 2027

Endorsed and approved by Assistant Principal Student Services & Careers

Date: September 2026

Shared for dissemination with the Senior Leadership Team

Date: September 2026

Jason Lancaster

Principal and CEO



Contents

1. INTRODUTION 3
2. CONTEXT 3
3. ROLES AND RESPONSIBILITIES 4
4. CODE OF CONDUCT 4
5. SYSTEM SECURITY 5
6. MAKING AN ALERT 5
7. MONITORING AND REVIEW 6
8. LINKS TO RELATED COLLEGE POLICIES / PROCEDURES 6
9. Appendices: 6
Appendix 1: EQUALITY & DIVERSITY IMPACT ASSESSMENT 7
Appendix 2: DATA PROTECTION IMPACT ASSESSMENT 9
Appendix 3: COMMUNICATIONS PLAN 11

1. INTRODUCTION

This E-Safety Policy applies to all members Northampton College, including students, staff, visitors and contractors who have access to, and are users of ICT systems and resources both in and out of learning venues, e.g. internet, electronic communications, Virtual Learning Environment (VLE) or mobile devices.

E-safety informs the wider safeguarding agenda, and this policy operates in conjunctions with other polices including Acceptable Use, Behaviour and Data Protection.

Where student access ICT through a third party (i.e. students on work placement or enrolled as an apprentice) the polices of the organisation should be followed.

2. CONTEXT

To prepare students for the needs of today and their future working lives where the curriculum and their personal goals require them to learn how to locate, retrieve and exchange information using a variety of technologies. Computer skills are vital to access employment and life-long learning as ICT is now seen as an essential skill for life. However, technologies present risks to vulnerable groups as well as benefits. Internet use for work, home, social and leisure activities is expanding across all sectors of society. This brings our staff and students into contact with a wide variety of influences some of which may be unsuitable. These new technologies are enhancing communication and the sharing of information, which inevitably challenge the definitions and boundaries of the college environment. Current and emerging technologies in college and more importantly, in many cases used outside the college by students include:

- Internet websites
- Virtual Learning Environments
- Artificial intelligence (A.I)
- Instant messaging
- Social networking sites
- E-mails
- Blogs
- Podcasting
- Video broadcasting sites
- Chat rooms
- Gaming and gambling sites
- Music download sites
- Mobile phones with camera and video functionality
- Digital cameras
- Smart phones, iPads and Tablets with e-mail and web applications.
- Microsoft Teams

All of these have potential to help raise standards of teaching and learning but may equally present challenges to both students and tutors in terms of keeping themselves safe. These challenges include:

- Exposure to inappropriate material
- Cyber-bullying via websites, social media, mobile phones or other technologies
- Identity theft or invasion of privacy

- Downloading copyrighted materials
- Exposure to inappropriate advertising online gambling and financial scams
- Safeguarding issues such as grooming (Children or vulnerable adults)
- Other illegal activities.

3. ROLES AND RESPONSIBILITIES

All teaching and non-teaching staff (including volunteers, suppliers, contractors and temporary staff) are responsible for supporting safe behaviour throughout the college and following safety procedures.

Staff

All college staff should:

- Participate in any mandatory e-safety training and awareness raising sessions read, understand, accept and act in accordance with the College E-Safety Policy report any suspicion of misuse to the designated persons or line manager.
- Refrain from making negative comments about students or Northampton College on any blogs or social networking sites. Negative comments such as these could be considered as gross misconduct as it potentially affects the reputation of the College and/or lowers morale.
- Help educate students in keeping safe, acting as a good role model in their own use of ICT and directing to sites which are appropriate for the use of learning.
- Be vigilant in monitoring the content of websites in case there is any unsuitable material
- Be aware of the potential for cyber-bullying in their sessions where malicious messages e.g. through the use of forums on the VLE and social networking sites, or via internal class emails or text messages on mobile phones etc, which can cause hurt or distress.

Students

Students are encouraged to access various technologies in sessions, private study and in the completion of assignments and independent research, and are therefore expected to follow the colleges Acceptable Use Policy. They should participate fully in e-safety activities and report any suspected misuse to a member of staff. Students are required to sign an agreement to state that they agree to the terms of our Acceptable Use Policy and their e-safety responsibilities:

4. CODE OF CONDUCT

Students & Staff are expected to:

- Behave in a safe and responsible manner.
- Treat equipment with respect.
- Store college data only on college authorised Cloud storage Microsoft One Drive for business.
- Be polite and not use e-mail, social media or blogs etc to make negative comments, bully or insult others.
- Use the resources only for educational purposes.

Students & Staff are expected not to:

- Waste resources including Internet and printers
- Eat or drink when using ICT resources
- Use someone else's login details or share your own
- Have any inappropriate files (e.g. copyrighted or indecent material)
- Attempt to circumvent or "hack" any systems
- Use inappropriate or unacceptable language
- Reveal their personal details or passwords
- Visit websites that are offensive in any way
- Use chat rooms or newsgroups, apart from the VLE Moodle site
- Do anything that could damage the reputation of the college
- Download anything inappropriate or install any unauthorised software.
- Store college data on any other cloud storage.

Breaching these Rules may lead to:

- Withdrawal from the College ICT facilities.
- Temporary or permanent prevention of access to the relevant pages on the Internet.
- Limited or disabled rights where systems are relevant.
- Appropriate disciplinary action under the college behaviour policy.
- Users should note that breaches of the provisions set out in these Rules may lead to criminal or civil prosecution.

5. SYSTEM SECURITY

Prior to commencing employment at Northampton College all users must read and agree to the college 'ICT Acceptable usage Policy'.

All IT equipment / computer systems are owned by Northampton College and have appropriate software/filtering to ensure safe internet use.

The college ICT Manager will be responsible for systems support and will ensure that the appropriate filters are applied to the equipment in the college.

If staff or students discover unsuitable sites have been accessed on the college IT equipment, they must report their findings to the ICT Manager so that filters can be reviewed.

Northampton College reserves the right to examine or delete any files that may be held on its system or to monitor any internet sites visited.

6. MAKING AN ALERT

Once you suspect or know of any e-safety issues, you should contact a Safeguarding Officer immediately.

7. MONITORING AND REVIEW

This Policy will be reviewed annually in line with the colleges quality systems.

8. LINKS TO RELATED COLLEGE POLICIES / PROCEDURES

- General Data Protection Policy and Procedure
- Child Protection - Safeguarding Children & Vulnerable Adults Policy 2026-27
- ITC Acceptable Use Policy
- Social Media Policy

9. Appendices:

- Appendix 1: EQUALITY AND DIVERSITY IMPACT STATEMENT
- Appendix 2: DATA PROTECTION IMPACT STATEMENT
- Appendix 3: COMMUNICATIONS PLAN

Appendix 1: EQUALITY & DIVERSITY IMPACT ASSESSMENT

This template has been designed to help you take action to improve services and practices which affect staff, students and other service users at Northampton College. By completing this template, you would have considered the impact that your policy, practice or service might have on particular social groups within the college community. The exercise will also provide you with the opportunity to demonstrate, where possible, that the College promotes equity, diversity and inclusion.
Once this Equality Impact Assessment has been created, please include on the last page of your policy document.

Policy Details	
What is the policy?	E-Safety Policy
Is it new or existing?	Existing
Department	Student Services
Policy Author (postholder title, name)	Mark Owen
Author of Equality Analysis	Mark Owen
Date of completion	1/9/2026

Aim and Objectives
Briefly describe the aims and objectives of the policy
The policy sets out the way in which the college manages e-safety within the college.

Policy Assessment				
Consider whether your policy might have an impact on various groups identified within the categories listed below and explain why you have reached this conclusion. Please tick (√) the identified level of impact (positive, negative, or no impact) and provide details of your findings.				
	Positive Impact	Negative Impact	No Impact	Findings
Race			x	
Religion and/or belief			x	
Sex (Gender)			x	
Gender Identity			x	
Disability			x	
Age			x	
Sexual orientation			x	
Marriage and/or civil partnership			x	
Pregnancy and/or maternity (including surrogacy and adoption)			x	

Other identified group (e.g. carers)			x	

Action Planning			
How do you intend to mitigate or eliminate any negative impact identified?	If a positive impact is identified, how do you intend to promote or develop this opportunity?	Where negative impact has been identified, can it be justified? If so, explain how.	How do you intend to mitigate or eliminate any negative impact identified?

Monitor and Review	
How will you monitor the impact of your policy once it has been put into effect?	
The policy will be monitored through feedback from services users gathered via: • Parents Survey • College Complaints Procedure	
Names and position of Impact Assessment Team (min of 3 preferably from areas across the College):	
Name	Position
Mark Owen	Assistant Principal - Student Services
Ashok Dave	Director of ICT Services
Jenny Thorpe	Assistant Principal – Teaching Learning and Quality
Equality Analysis Sign-Off Signature and Date: 01/09/2026	
Review Date:01/09/2027	

Appendix 2: DATA PROECTION IMPACT ASSESSMENT

Data Protection Impact Assessment

Does this Policy

- require the collection and use of data in addition that normally collected by the College?

Yes / No (if Yes complete Assessment point number 1)

- require the sharing of data with partners?

Yes / No (if Yes complete Assessment point number 2)

1. Is additional data being collected? If so please detail:

No

Is data collected personal and/or sensitive?

N/A

How will you collect, use, store and delete data?

N/A

2. Will you be sharing data with anyone? Please detail what data, with who and confirm a **Data Sharing Agreement** is in place

No

Describe the purposes of the processing / sharing: What are the benefits of the processing/ sharing – for you, and more broadly?

N/A

Consider how to consult with relevant stakeholders: describe when and how you will seek individuals' views – or justify why it's not appropriate to do so.

N/A

Describe compliance and proportionality measures, in particular:
What is your lawful basis for processing?

N/A

How will you ensure data quality and data minimisation?

N/A

What information will you give individuals?

N/A

Please attach a Risk Assessment if there are significant risks to data protection

Signed by Data Protection Officer

Name: Rav Garcha

Date: September 2026

Appendix 3: COMMUNICATIONS PLAN

Version	Final
Ratified by	Policy & Strategy Group
Date Ratified	1st September 2026
Date Issued	1st September 2026
Expiry Date	1st September 2027
Lead Manager	Mark Owen
Name of Author	Mark Owen
Audience	College Staff, Applicants
Communication Plan	College Staff, Applicants, College Website