Doncaster College | University Centre

North Lindsey College

DN COLLEGES GROUP

E-Safety Policy

1. Purpose

1.1 The purpose of this policy is to ensure that DN Colleges Group and all its subsidiaries (hereafter referred to as 'the College') provides a framework for E-Safety to ensure that appropriate safeguards and processes are in place.

1.2 This policy is written in line with the College's Strategic Plan, Vision and Values which identify a commitment to safeguarding, health, safety and welfare, equality diversity and inclusion and data protection.

1.3 The College recognises the benefits and opportunities that new technologies afford teaching, learning and assessment. The global nature of the internet, Artificial Intelligence (AI) and the variety of technologies now available, mean that we need to implement safeguards that enable students, apprentices, staff, volunteers and visitors to identify and manage risks associated with their use.

1.4 The College is committed to fostering a culture where colleagues feel comfortable talking about E-Safety, recognise E-Safety matters and report concerns they may have. Our goal is to provide guidance and support to empower staff and students to use modern technologies in an engaging and motivating manner, while also promoting safe practices.

2 Scope

2.1 This policy applies to all applicants, enrolled students, both FE and HE, irrespective of age, including Apprentices, Adults, whether full-time, part-time or distance learners (hereafter referred to as students).

2.2 This policy applies to all staff, paid and non-paid, including agency workers, contractors, volunteers and governors (all of whom will hereafter be referred to as 'Staff'). The scope of this policy includes the children of adults who use our services. This policy also applies to visitors and those who use our facilities.

2.3 We have a responsibility to promote E-Safety to our students, in particular children, young people and vulnerable adults, to keep them safe and to work in a way that protects them. Some students may be additionally vulnerable because of previous experiences, communication needs and/or other issues so additional safeguards may be needed.

2.4 Technology can facilitate learning and development in addition to accessing opportunities and information. However, it can also present a window to potential or actual harm or abuse.

The scope of this policy refers to several situations including, but not limited to, E-Safety in the following contexts:

- Students and staff using College devices and/or College Wi-Fi
- Students and staff using their own devices on college sites
- Online behavior of students and staff, whilst on or off site
- Visitors and those who hire our facilities using College devices and/or College Wi-Fi

2.5 The College will utilise systems to monitor network usage and E-Safety. Details of which are provided in the Acceptable use Policy for IT systems.

3 Responsibilities

3.1 E-Safety is everyone's responsibility. All staff and volunteers have a responsibility to access, read and understand the E-Safety Policy. All staff will receive appropriate E-Safety Training at induction which will be updated at least annually. Staff will access periodic and regular updates.

3.2 Students are responsible for using the College digital technology systems in accordance with the Acceptable Use Agreement and E-Safety Policy, which can be found on the Staff Intranet. This includes personal devices when permitted.

3.3 All staff must report any worries, concerns or issues in a timely manner in accordance with this policy and the Safeguarding and Child Protection policy. Any worries, concerns or issues must be reported to a Designated Safeguarding Lead (DSL) using the College procedures for reporting concerns. Additional guidance for reporting can be found in the E-Safety Handbook for Staff.

3.4 Staff have a responsibility to ensure students follow the E-Safety policy. Curriculum and curriculum support staff have a responsibility to integrate online safety into the curriculum. Curriculum and Academic Services staff have a responsibility to ensure everyone utilising College systems adheres to copyright laws. Staff must supervise the use of digital technologies in lessons and guide students to appropriate websites and have a zero-tolerance approach to online bullying. All curriculum staff must ensure students know how to report any worries, concerns or issues.

3.5 Leaders and managers have a specific responsibility to ensure that they, and their staff, are fully aware of this policy and that it is applied in accordance with the procedures noted in the E-Safety Handbook for Staff, visitors' guidance and premises hire processes as appropriate.

3.6 The Designated Safeguarding Lead (DSL) takes lead responsibility for Safeguarding and Child Protection. The DSL will complete relevant and regular training in E-Safety to understand the associated risks and will have the necessary knowledge regarding online safety. The DSL, and the deputies they appoint, are responsible for responding to reports of online safety incidents or concerns. The DSL will liaise with other colleagues and external providers on matters of E-safety, including digital and technical support.

3.7 The Personal Development Team deliver and facilitate E-Safety education and learning to equip students with the knowledge and skills to navigate the digital world safely.

3.8 The IT Infrastructure Team and the Business Systems and Information Team are responsible for monitoring College systems and infrastructure to endeavour they remain secure and protected from misuse and malicious attacks. Network usage is monitored to prevent misuse. Filtering and monitoring systems are maintained by these teams.

3.9 The Academic Services team is responsible for developing online and offline training resources for staff and students in relation to E-Safety. They work collaboratively with the Safeguarding Team to deliver E-Safety training for staff, ensuring that all staff are equipped with the knowledge needed to maintain a safe online environment. They also provide support to the Personal Development team, with necessary content, updates and resources to facilitate E-Safety education for students.

3.10 The College Data Protection Officer has a responsibility to ensure that the College processes the personal data of its staff, students, customers, providers or any other individuals (also referred to as data subjects) in compliance with the applicable data protection rules.

4 Definitions and/or Relevant Legislation

4.1 E-Safety and risks

E-Safety is the awareness, practice and training of individuals, together with IT infrastructure and security to ensure the safe use of online technologies, therefore maintaining both physical and psychological wellbeing as well as organisational reputation.

E-Safety risks are collectively known as the 4 Cs of online safety.

Content: Inappropriate material available online including adverts, spam, sponsorship, violent or hateful content, pornographic or unwelcome sexual content, biased materials, racist materials and misleading information or advice.

Contact: Contact from someone online who may wish to bully or abuse. This could also include online grooming, online harassment, or activities of a commercial nature, including tracking and harvesting personal information.

Conduct: A person may be the perpetrator of activities including illegal downloading, hacking, gambling, financial scams, bullying or harassing another. They might create and upload inappropriate material or provide misleading information or advice.

Commerce: risks associated with online gambling, phishing or financial scams.

4.2 Online abuse

The NSPCC definition of online abuse is as follows: “Online abuse is any type of abuse that happens on the web, whether through social networks, playing online games or using mobile phones” (NSPCC, 2019). Further detail can be found in the E-Safety Handbook for Staff.

4.3 Relevant legislation and guidance include, but is not limited to:

- Online Safety Act (2023)
- Computer Misuse Act (1990)
- Malicious Communication Act (1998)
- Keeping Children Safe in Education (2024) and any subsequent amendments or updates
- Prevent Duty Guidance (2023) and any subsequent amendments or updates
- Working Together to Safeguard Children (2023)
- Equality Act (2010)
- Data Protection Act (2018) and UK GDPR

This policy should be read in conjunction with the E-Safety Handbook for Staff, visitors guidance and premises hire processes.

5 The Policy

5.1 Education and Training for staff

Effective education and training are crucial components of our E-safety policy, ensuring that all staff are equipped with the knowledge and skills to navigate the online world safely and responsibly and to support students. All new staff members receive E-safety training as part of their induction process, including modules delivered online. Regular training sessions are delivered to update staff on the latest E-safety issues, trends, and best practices. Staff have access to a range of E-safety resources and support from the Academic Services Team.

5.2 **Education and Training for students**

E-Safety education is integrated into the curriculum through Personal Development sessions and in subject areas. This ensures that students receive consistent messages about E-Safety. Students have access to a range of E-safety resources, including guides, and online tools including a range of sources of support.

5.3 **E-Safety information for Parents/Carers**

Parents and carers have a key role in fostering safe online practices. To support them, we offer up-to-date information and resources on E-Safety. We encourage parents and carers to engage with the College E-safety initiatives available on our website.

5.4 **Resources**

The College will seek E-Safety advice and use resources from UK organisations such as UK Safer Internet Centre, Internet Matters, NSPCC and CEOP. E-Safety advice and guidance will be displayed on college sites.

5.5 **Acceptable and Unacceptable Behaviour**

All users of college digital technology systems are expected to adhere to the following standards of behaviour.

- All interactions online should be conducted with respect and consideration for others. This includes avoiding any form of online harassment, bullying, or discrimination.
- It is unacceptable to download or transmit any material that is obscene, abusive, sexist, racist, defamatory, related to violent extremism or terrorism, or intended to annoy, harass, or intimidate another person. This also applies to the use of social media accessed from college systems.
- Users must comply with all relevant laws and regulations, including those related to data protection, copyright, and computer misuse.

5.6 **Use of Images and Video**

The use of images and videos can significantly enhance teaching and learning experiences. However, it is essential to ensure that their use complies with legal requirements and respects the privacy and rights of individuals. The Use of Images and Video guidelines are detailed in the E-Safety Handbook for Staff.

5.7 **Use of Personal Devices**

Staff and students should avoid using personal devices to capture images or videos for college purposes. If personal devices are used in exceptional circumstances, ensure that the content is transferred to a college system and deleted from the personal device immediately. Visitors must be informed of the College policy on the use of images and videos.

5.8 **Artificial Intelligence (AI)**

Due to the rapid developments in AI, additional guidance has been developed which includes reference to using AI safely and effectively. The guidance should be read in conjunction with this policy.

5.9 **E-safety Concerns**

Concerns could refer to online bullying, sharing inappropriate content, online harassment, or any other online safety issues. Further detail can be found in the E-Safety Handbook.

All worries, concerns or issues must be reported to the Safeguarding Team. Students may report worries, concerns or issues to other staff who will then escalate these to the

Safeguarding Team. Students can also report bullying, harassment and victimisation using the online reporting tool on the College website.

All staff must know how to report E-Safety issues according to the Safeguarding and Child Protection policy. Further detail can be found in the E-Safety Handbook.

5.10 **Data Protection**

The College is committed to ensuring the privacy and protection of all personal data. We adhere to the principles outlined in the Data Protection Act (2018) and UK GDPR, ensuring that all personal information is handled securely and responsibly. For detailed guidelines and procedures, please refer to our Data Protection Policy.

6 Relevant Policies and Procedures

6.1 Relevant Policies include, but are not limited to:

- Data Protection Policy
- Digital Communications Policy (Formerly Social Media Policy)
- IT policies and procedures for students, staff and visitors including Acceptable use for IT systems, Bring Your Own Device (BYOD) and IT Security Policy.
- Equality, Diversity and Inclusion Policy
- Safeguarding and Child Protection Policy
- DNCG Behavioural Policies and procedures for students, staff and visitors including the Prevention from Bullying, Harassment and Victimisation Policy
- DN Colleges Group Generative Artificial Intelligence Principles

7 Who to contact with Queries

7.1 For advice or guidance on any of the topics covered in this policy contact:

- Safeguarding Team safeguarding@dncolleges.ac.uk
- Academic Services help.academicservices@dncolleges.ac.uk
- HR Team hr.group@dncolleges.ac.uk

7.2 It is recognised that managing disclosures, incidents or concerns may be stressful for staff. For additional support and guidance, staff may contact a member of the HR team or access the Employee Assistance Programme.

7.3 The policy and procedure will be monitored by the People Services Department.

If you require this information in another language or a different format, please contact Academic Services academic-services@dncolleges.ac.uk or hr.group@dncolleges.ac.uk.

8 Communication

8.1 The E-Safety Policy will be made available via the Intranet site, website and from the HR Team.

9 Authorisation

Policy Holder:	Rachel Maguire - Chief Operating Officer - People & Information
Union Approval & Date:	(if applicable)
SLT Approval & Date:	9 October 2024
Governor Committee/ Board Approval:	(if applicable)
Next Review Date:	October 2027

*Policies will be reviewed every 3 years unless there is a specific requirement to undertake a review more frequently. If for any reason a review does not take place in the planned period, the policy will remain current until a review takes place.

The Equality Impact has been considered on this policy and procedure.