Online Safety Policy(v1) 2023

North Warwickshire and South Leicestershire College

Policy Author: Assistant Principal Student Services and Support

Lead Owner: Assistant Principal Student Services and Support

Target Audience: Staff / Student / Public

Policy Location: Website / HR SharePoint / Staff SharePoint

Contents

Online Safety Policy(v1) 2023

Page

1. Introduction 1
2. Definitions 1
3. Related Policies, Procedures and Documents 1
4. Rationale 1
5. Roles and Responsibilities 2
6. Core Principles 3
7. Equality Analysis 8
8. Data Protection Impact Assessment 9
9. Implementation, Monitoring and Review 9

Document History

Version Number	Amended By	Date of Revision	General Revision Description
V1			New Policy

Online Safety Policy (v1) 2023

1. Introduction

1.1 This Policy applies to all staff, students, apprentices and other College users, including volunteers, external contractors, distance learning students, and employers where students and / or apprentices have work placements or are engaged in work-based learning.

1.2 Online Safety forms part of the Safeguarding Policy, with this policy providing specific guidance around the risks associated with online activity and a framework with which to protect all College users from potential harm online.

1.3 Thus Policy applies to all who have access to the internet and the use of technology, including personal devices, or where students, apprentices, staff, or other individuals have been provided with College issued devices for use off-site, such as work laptops, tablets, or mobile phones. The College recognises that in some cases online risks will be minimised by enforcing expectations around behaviour and codes of conduct, alongside teaching and learning in relation to online safety, and that not all risks can be flagged to the Safeguarding Team through web-filtering and monitoring. Web filtering e.g. blocking access to certain sites and content is active for all College devices. Keyword monitoring is only on College owned devices.

2. Definitions

2.1 Web-filtering is the process of screening and/or restricting users from accessing objectionable, harmful or dangerous web content

2.2 Key word monitoring captures activity that may indicate a risk through user activity online through web browsers or offline in platforms such as Microsoft Word. This is also active in the College application “My NWSLC”.

3. Related Policies, Procedures and Documents

3.1 Safeguarding and Protecting Children and Vulnerable Adults Policy 2023.

3.2 Student Conduct Expectations Policy 2023.

3.3 IT Acceptable Use Policy 2023.

3.4 NWSLC (North Warwickshire and South Leicestershire College) Prevent Strategy 2023.

3.5 Anti-Bullying Policy 2023.

3.6 Other policies and documents may be identified from time to time as circumstances change and may be added to this list.

4. Rationale

4.1 The Policy aims to ensure that:

i. Members of the North Warwickshire and South Leicestershire College community are safeguarded and protected whilst engaged in online activity.

ii. There is a commitment across the College to identify and embed approaches to educate and raise awareness of online safety.

iii. Staff work safely and responsibly to role model positive behaviour online and to manage professional standards and practice when using technology.

iv. The College is effective in responding to online safety concerns.

4.2 The College identifies that the issues classified within online safety are considerable but can be broadly categorised into three areas:

i. **Content:** being exposed to illegal, inappropriate or harmful material.

ii. **Contact:** being subjected to harmful online interaction with others.

iii. **Conduct:** personal online behaviour that increases the likelihood of, or causes, harm

5. Roles and Responsibilities

5.1 The Designated Safeguarding Lead (DSL) and deputies have lead responsibility for safeguarding and child protection, including online safety. However, all members of the College community have a significant role to play with regards to online safety.

5.2 The Designated Safeguarding Lead and assigned Deputies will:

i. Act as a named point of contact for all online safety issues.

ii. Work closely with the IT Director and IT Services team to ensure effective systems are in place and complete checks on the filtering and monitoring systems at least annually.

iii. Work alongside curriculum colleagues to ensure online safety is recognised as part of the College's safeguarding responsibilities and that a coordinated approach is implemented.

iv. Ensure that all members of staff access regular, up-to-date, and appropriate safeguarding training which includes online risks.

v. Access regular and appropriate training and support around the additional online safety risks faced by students and apprentices with special educational needs and disabilities (SEND).

vi. Keep up to date with current research, legislation, and trends regarding online safety and communicate this as appropriate.

vii. Work with staff to coordinate participation in local and national events to promote positive online behaviour, such as Safer Internet Day.

viii. Ensure that online safety is promoted to staff, students, apprentices, parents, carers and the wider community through a variety of channels and approaches.

ix. Maintain records of online safety concerns, including actions taken, as part of the College's safeguarding recording mechanisms.

x. Monitor online safety incidents to identify gaps and trends and use the data to update the College's educational response, policies, and procedures.

xi. Report online safety concerns to the Senior Leadership Team and Safeguarding Taskforce via safeguarding reporting.

xii. Meet regularly (termly) with the governor with lead responsibility for safeguarding.

5.2 The Executive Team and Senior Leadership Team will:

i. Ensure that online safety is viewed as a safeguarding issue and that practice is in line with national and local requirements and recommendations.

ii. Ensure that there are appropriate and up-to-date policies in place regarding online safety, including a staff code of conduct, student code of conduct and IT acceptable use policy.

iii. Ensure that online safety is embedded in curriculum delivery to enable all students and apprentices to develop an age and level appropriate understanding of online safety.

iv. Support the DSL and deputies by ensuring that they have sufficient time and resources to fulfil their online safety responsibilities.

v. Ensure that there are robust reporting channels for the College community to access regarding online safety concerns, including internal, local, and national support.

vi. Audit and evaluate online safety practice to identify strengths and areas for improvement.

5.3 IT Services will:

i. Ensure that suitable, robust, and appropriate filtering and monitoring systems are in place and updated regularly.

ii. Provide technical support to the DSL and Senior Leaders, especially in the development of appropriate online safety policies, procedures, and monitoring processes, to allow them to take appropriate safeguarding action where required.

iii. Work closely with the DSL and deputies to ensure effective systems are in place, data is provided and checks on the filtering and monitoring systems are completed at least annually.

iv. Proactively manage the IT infrastructure to ensure that this is as safe as is reasonably practicable against misuse or malicious attack, whilst allowing learning opportunities to be maximised.

5.4 All staff have a responsibility to:

i. Read and adhere to the Online Safety Policy, IT Acceptable Use Policy and any associated guidance.

ii. Take responsibility for the equipment they use and the data they have access to.

iii. Model good practice when using technology and maintain a professional level of conduct in their personal use of technology, both on and off site.

iv. Embed online safety education within curriculum delivery, wherever possible.

v. Have an awareness of a range of online safety issues and how they may be experienced by the College's students and apprentices.

vi. Identify online safety concerns and take appropriate action by following the College's Safeguarding reporting procedures.

5.5 All students and apprentices have a responsibility to:

i. Take responsibility for the equipment they use and the data and information they have access to.

ii. Adhere to the College's Code of Conduct and act responsibly when using online platforms for communication, for educational research, educational activities, and assessment.

iii. Participate in College activities to further develop knowledge and understanding of online risks.

iv. Report any suspicious online activity to a staff member, be that teaching staff, the IT department, or the Safeguarding team.

v. Report any concerns they have for themselves or others through the College's Safeguarding "Log a Concern" Procedure

6. Core Principles

6.1 The College recognises that online safety is an essential part of safeguarding and acknowledges its duty to ensure that all students and apprentices are protected from potential harm online, whilst also recognising that the internet and associated devices such as computers, tablets, laptops, mobile phones, and games consoles are an important part of everyday education and life. The College believes that students and apprentices should be empowered to build resilience and to develop strategies to manage and respond well to online risk.

6.2 Students and apprentices will be supported to:

i. Engage in age, curriculum and level appropriate online safety education opportunities.

ii. Contribute, as appropriate, to the development of online safety policies.

iii. Read and adhere to the IT Acceptable Use Policy and the Student Code of Conduct.

iv. Respect the feelings and rights of others both on and offline.

v. Take responsibility for keeping themselves and others safe online.

vi. Seek help from a trusted adult if there is an online safety concern and support others who may be experiencing online safety issues.

6.3 Corporation Members and College Senior Leaders, in conjunction with IT Services, the Designated Safeguarding Lead (DSL) and Curriculum Leadership Teams, have ensured that the College has age and ability appropriate filtering and monitoring in place to limit students' and apprentices' exposure to online risk whilst on College premises. The Senior Leadership Team will ensure that regular checks are made to confirm the effectiveness and appropriateness of the College's approach.

6.4 Corporation Members and Senior Leaders are aware of the need to prevent "over-blocking" as this may unreasonably restrict what can be taught with regards to online activities and safeguarding.

6.5 **Managing Internet Access**

Staff, students, apprentices, and visitors will be signposted to the IT Acceptable Use Policy on first use of College systems, and the policy's Simplified Code will be regularly promoted across the College community.

6.6 **Filtering**

The College uses an appropriate filtering system which blocks sites that are deemed to be harmful, distracting, or unnecessary for the fulfilment of a complete learning experience and blocks all sites on the Internet Watch Foundation (IWF) list.

Whilst the filtering system will be updating constantly and uncategorised sites will be blocked, the College acknowledge that no system is fool proof. As such, staff, students, apprentices, and visitors are encouraged to report unsuitable sites that are discovered to be accessible to IT Services.

Any material believed to be illegal will be reported immediately to the appropriate agencies, such as the IWF, Police, or the Child Exploitation and Online Protection Command (CEOP).

6.7 **Monitoring**

Internet usage is appropriately monitored on all College provided internet enabled devices, in line with data protection, human rights, and privacy legislation. Any identified concern is reviewed by the DSL or nominated deputy in line with the College's Safeguarding Procedures.

6.8 **Use of Personal Devices and Mobile Phones**

The College recognises that personal communication through mobile technologies is an accepted part of everyday life for students, apprentices, staff, and other members of the wider College community, but that technologies need to be used safely and appropriately within the College setting.

Members of staff should adhere to the IT Acceptable Use Policy and the Staff Code of Conduct in their use of personal devices and mobile phones on College premises. Personal devices may be used for College related communication but College software and College identification should always be used.

Staff must never communicate with a student through their own personal contact number, email, or other personal profile.

Students can be contacted via their approved contact details provided at enrolment or through College assigned software and identification such as their College email address, teams or APP profile.

Safe and appropriate use of personal devices and mobile phones will form part of the educational approach to students and apprentices across the College. All students and apprentices are expected

to adhere to the Student Code of Conduct and any locally issued classroom management instructions in their use of personal devices and mobile phones.

6.9 **Social Media**

North Warwickshire and South Leicestershire College will control student and staff access to social media whilst using College provided devices and systems on-site. Access to social media platforms is universally blocked by College systems for personal use. Limited access is permitted for the purpose of marketing and promotion of College activities.

The College expects all members of staff to use social media safely and responsibly. Concerns regarding staff conduct on social media platforms should be raised with the Human Resources Team. Where the concern is of a safeguarding nature a report should be made to the DSL as detailed in the College's Safeguarding Policy and Procedures.

Safe and appropriate use of social media will form part of the educational approach to students and apprentices across the College Group. Students and apprentices will be advised:

i. To consider the benefits and risks of sharing personal details on social media platforms that could identify them or their location.

ii. To only approve and invite known friends on social media sites and to deny access to others by making profiles private.

iii. That they should not meet online friends without giving proper consideration to their personal safety and where under 18 informing a trusted adult.

iv. To use passwords on all social media accounts.

v. To never give access to their account to another person.

vi. To only use social media sites that are appropriate for their age and ability.

vii. How to block unwanted communications.

viii. How to report concerns to both the College and external agencies.

Any concerns regarding student or apprentice conduct on social media should be approached following guidance in the appropriate policy:

i. Safeguarding and Protecting Children and Vulnerable Adults Policy 2023.

ii. Student Code of Conduct.

iii. Student Conduct Expectations Policy 2023.

iv. Anti-Bullying Policy 202.3

Organisational use of social media is guided by the internal policies and procedures of the Marketing Team. This includes setting up social media groups using the College name and those intended to promote the College offer. All staff should seek advice and guidance from the Marketing Team (marketing@nwslc.ac.uk) prior to the instigation of any organisational social media use.

6.10 **Safer Use of Technology in the Learning Environment**

The College uses a wide range of technology in the delivery of its services. This includes, but is not limited to:

i. Computers, laptops, tablets, and other digital devices.

ii. Learning platforms including but not limited to Moodle and Smart Assessor.

iii. Email, the My.NWSLC App and other communication systems.

iv. Games consoles and other games-based technologies.

v. Digital cameras, web cameras, video conferencing systems, and video cameras.

All devices provided by the College will be used in accordance with the IT Acceptable Use Policy and with appropriate safety and security measures in place. All internet connected devices, including College issued mobile phones, will be managed using mobile and other device management software.

Members of staff will always evaluate websites, online resources, tools, and apps fully before use in the learning environment or recommendation for home use.

The College will take necessary steps to ensure that search tools provided are appropriate, for example enforcing safe search when using Google.

6.11 **Teaching and Learning of Online Safety**

The College will establish and embed a progressive online safety curriculum to raise awareness of responsible internet use amongst students and apprentices by:

i. Ensuring initial education regarding safe and responsible internet use occurs during student induction and within the first six weeks of each new academic year.

ii. Ensuring ongoing online safety education is embedded within programmes provided by curriculum and pastoral teams.

iii. Reinforcing online safety messages when technology or the internet is used.

iv. Educating students and apprentices of all ages and levels in the effective use of the internet to research, including the skills of knowledge location, retrieval, and evaluation.

v. Educating students and apprentices to be critically aware of the materials they read and supporting students and apprentices to learn how to validate information before accepting its accuracy.

The education described above will be flexible and differentiated between learning programmes where altered, more specific, or less intensive delivery is required. Specialist technical support will be provided to groups where more significant access to the internet and/or technology is required and where this would ordinarily be restricted.

Students and apprentices will be supported to understand the acceptable use of IT facilities in a way that suits their age and ability by:

Having access to the IT Acceptable Use Policy in central areas such as the Box, Moodle, and Smart Assessor.

i. Informing students and apprentices that network and internet usage will be monitored for safety and security purposes in accordance with relevant legislation.

ii. Ensure staff are on hand to explain this policy to students and apprentices.

6.12 **Vulnerable Learners**

The College recognises that some students and apprentices are more vulnerable online due to a range of factors including, but not limited to:

i. Children in care.

ii. Care leavers.

iii. Students and apprentices with special educational needs and disabilities (SEND).

iv. Students and apprentices with mental health needs.

v. Students and apprentices with English as an additional language (EAL).

vi. Students and apprentices experiencing trauma or loss.

When developing and implementing online safety education, specialist support will be sought from staff, including those responsible for safeguarding, mental health, and SEND.

6.13 **Awareness and Engagement with Parents/Carers of Students under 18 or those with an Education, Health, and Care Plan (EHCP)**

The College recognises that parents and carers have an essential role to play in enabling young people to become safe and responsible users of the internet and associated technologies.

The College will, where appropriate:

i. Provide information relating to pertinent issues around online safety to the parents/carers of students under 18/those with an EHCP.

ii. Publish the Online Safety Policy on the College website and publicise online safety messages on social media channels.

iii. Encourage parents/carers to read the College's IT Acceptable Use Policy.

6.14 **Training and Engagement with Staff**

As part of wider induction activity new staff are made aware of the Safeguarding Policy and Procedures, including the Online Safety Policy.

New and existing staff will be made aware that:

i. IT systems are monitored, and activity can be traced back to individual users. Staff will be reminded to behave professionally and in accordance with College policies when accessing College systems and devices.

ii. Online conduct outside of the setting, including personal use of social media, could have an impact on their professional role and reputation.

iii. New resources and tools will be highlighted and developed for staff to use with students and apprentices.

iv. The procedure to follow regarding online safety concerns affecting students, apprentices, colleagues, or other members of the College Group community.

6.15 **Managing Email**

The College's email system will be managed in line with data protection legislation and other internal policies, such as the IT Acceptable Use Policy, IT Security Policy, and Code of Conduct.

i. The forwarding of chain messages is not permitted.

ii. Spam or junk mail should be placed in the appropriate 'Junk Email' folder.

iii. Suspicious emails should be reported to IT Services

iv. College generated email addresses should not be used to set up logins for personal websites such as social media or shopping.

The receipt of any offensive communication should be reported immediately to the recipient's Personal Tutor (if received by a student/apprentice) or Line Manager (if received by a member of staff). When safeguarding is a factor, the DSL or nominated deputy should be notified immediately.

Members of staff are encouraged to have an appropriate work/life balance when checking and responding to email, especially when communicating with students, apprentices, and parents/carers outside of normal working hours. Staff are advised to not have contact with external agencies, students, apprentices, or parents/carers outside of normal working hours.

6.16 **Management of College Platforms**

The College uses a number of learning platforms and other software packages to enhance the student experience, diversify learning and enable the tracking of student and apprentice progress, including:

i. Smart Assessor.

ii. Moodle.

iii. The Box.

iv. E-Assessor.

v. My.NWSLC App.

The College may, as part of its normal business practices, choose to adopt new platforms, replace existing platforms with an appropriate substitute, or cease using a platform altogether.

The use and content of learning platforms will be monitored, different methods are implemented to monitor the use of these platforms.

Only current members of staff and students/apprentices will have access to learning platforms. Accounts are disabled once a member of staff or student/apprentice leaves the College.

All tracking systems holding student or apprentice data, images, videos, or other digital information are risk assessed prior to use, and on an ongoing basis, to ensure that all information is stored securely and in accordance with data protection legislation.

6.17 **Reducing Online Risks**

The College recognises that the internet is a constantly changing environment with new apps, devices, websites, and material emerging at a rapid pace.

We will:

i. Regularly review the methods used to identify, assess, and minimise online risk.

ii. Examine emerging technologies for educational benefit and undertake appropriate risk assessment before any new technology is used within the College.

iii. Ensure that appropriate filtering and monitoring is in place and take all reasonable precautions to ensure that users can only access appropriate material.

iv. Recognise that due to the global and ever-changing nature of the internet it will not always be possible to ensure that unsuitable material cannot be accessed via the College's systems and networks but take reasonable precautions to ensure that unsuitable material is reported.

All members of the College community are made aware of our expectations regarding safe and appropriate online behaviour and the importance of not posting any content, comments, images, or videos which could cause harm, distress, or offence to members of the College community.

6.18 **Responding to Online Concerns**

All responses to concerns raised will be managed within the provisions set out within the College's Safeguarding Policy and/or Anti-Bullying Policy. Concerns may include:

i. Student or apprentice welfare.

ii. Online sexual violence and/or sexual harassment between children.

iii. Youth produced sexual imagery.

iv. Online child sexual abuse and exploitation.

v. Indecent images.

vi. Cyberbullying.

vii. Online hate.

7. Equality Analysis

7.1 By virtue of the provisions of the Equality Act 2010, the College has a duty to have due regard to the need to:

i. eliminate unlawful discrimination, harassment and victimisation and other prohibited conduct.

ii. advance equality of opportunity between people of different groups.

iii. foster good relations between people from different groups.

7.2 In implementing this Policy and associated procedures, the College will actively take these aims into account as part of its decision-making process and will demonstrate how this has been undertaken.

7.3 Where necessary a full equality impact assessment will be undertaken.

8. Data Protection Impact Assessment

8.1 Data Protection Impact Assessments (DPIA) are an essential part of the College's accountability obligations under the UK GDPR. Conducting a DPIA is a legal requirement for any type of processing, including certain specified types of processing that are likely to result in a high risk to the rights and freedoms of individuals. Under UK GDPR, failure to carry out a DPIA when required may leave the College open to enforcement action.

8.2 A DPIA, relating to any relevant areas within this Policy and Procedure, will therefore be undertaken to enable the systematic analysis, identification and minimisation of data protection risks and to demonstrate how the College complies with its data protect obligations.

9. Implementation, Monitoring and Review

9.1 This Policy will be reviewed every three years, or as otherwise required by law, regulation, organisational policies, good practice, or contractual obligations.