Online Safety Policy
2022 – 2024

Introduction

1. West Nottinghamshire College recognises the opportunities that technology offers to teaching, learning, engagement and communication. Our technology enhanced learning and digital strategy (TELD) sets out our ambition to fully utilise the potential of technology to enhance skills and promote achievement.

2. However, the accessible and global nature of the internet and the variety of technologies available mean that we are also aware of potential risks and challenges associated with such use. Our approach is to implement safeguards within the College and to support staff and learners to identify and manage risks independently. We believe this can be achieved through a combination of security measures, training and guidance and the implementation of our associated policies.

3. Our duties enshrined within keeping children safe in education require us to do all we can to ensure that our students stay safe online and further, ensure they are equipped with an understanding of risk, resilience and personal strategies to keep themselves safe online.

4. Our online safety policy should be read in conjunction with the following policies, procedures and guidance notes: safeguarding policy and procedure; bullying and harassment policy (students); IT acceptable use policy; positive behaviour management pack and student code of conduct; email etiquette guidance (staff); staff code of conduct; and staff social media policy.

Scope

5. This policy covers:

    - Anyone logging into any network, service, website or portal associated with West Nottinghamshire College.
    - Connecting a device via the West Nottinghamshire College network.
    - Any electronic communication with a West Nottinghamshire College student, member of Staff or contractor.
    - From any geographic location both on Campus and off Campus.

Definitions

6. In setting out the definitions related to online safety the college uses the 4 Cs outlines within keeping children safe in education which have been incorporated into the college's safeguarding processes and procedures:

    - Content – being exposed to illegal, inappropriate or harmful content for example pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism;

- Contact – being subjected to harmful online contact and interaction with other users, for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom and exploit them for sexual, criminal, financial and other purposes;
- Conduct – online behaviour that increases the likelihood of harm for example, making and sharing of nudes/semi-nudes, pornography, sharing explicit images and cyber bullying; and
- Commerce – educating students to the range of online risks including gambling, inappropriate advertising, phishing and scams.

Responsibilities

7. **All staff** are responsible for ensuring the safety of students online and for ensuring their own conduct is appropriate and does not put students at risk of harm.

8. **All staff** are responsible for reporting any concerns about students to the safeguarding team in line with the college's procedures;

9. **The designated safeguarding lead** is responsible for ensuring that appropriate training is provided to all staff in relation to online safety and that appropriate action is taken to safeguard students when concerns arise;

10. **The vice principal curriculum and quality** is responsible, through the tutorial programme for ensuring students have appropriate and meaningful training around online safety;

11. **The director of IT, estates and learning resources** is responsible for ensuring appropriate and effective filtering and monitoring systems are in place;

12. **Governors** are responsible for ensuring that appropriate measures are in place and are effective in keeping students and staff safe online; and

13. **All students** are responsible for ensuring their own conduct does not put others at risk or harm and for reporting any concerns they may have about online safety.

Monitoring

14. West Nottinghamshire College actively monitor, log and report on students and staff use of IT systems and IT network usage as part of our safeguarding and prevent duties. This includes the use of filtering systems and the use of Smoothwall to monitor activity on college devices.

15. An attempt to interfere or avoid the monitoring or logging of any IT systems will be referred to the college's disciplinary process. Where requested this information will be securely shared with appropriate local authorities and external support agencies.

Training

16. Students will be provided with online safety guidance at induction by personal tutors, this includes the proper use of college systems. Tutorial planning will include appropriate and

relevant online guidance for students. Tutorials will also ensure students consider their digital footprint in both a personal and professional context.

17. Issues associated with online safety apply across the curriculum and students should receive guidance on what precautions and safeguards are appropriate when making use of the internet and mobile technologies. Students should also know what to do and who to talk to where they have concerns about inappropriate content, either where that material is directed to them, or where it is discovered as part of a random search. Within classes, students will be encouraged to question the validity and reliability of materials researched, viewed or downloaded. They will also be encouraged to respect the copyright of other parties and to cite references properly.

18. Staff will receive an introductory session for digital learning/working systems and environments within the induction period. This introductory session will signpost appropriate policies and procedures. Any new or temporary users will also be asked to sign the college's IT acceptable use policy.

Behaviour

19. Communications by staff and learners should be courteous and respectful at all times whether offline or online. Any reported incident of bullying or harassment or other unacceptable conduct will be treated seriously and in line with the Anti-Bullying and Harassment processes (staff and students).

20. Cyber bullying is a form of bullying. As it takes place online, it is not confined to college buildings or college hours. Cyber bullies can communicate their messages to a wide audience with speed and often remain anonymous or unidentifiable.

21. Cyber bullying includes bullying via:

    - Text message and messaging apps e.g. sending unwelcome texts or messages that are threatening or cause distress.
    - Picture/video-clips e.g. using mobile device cameras to bully someone, with images usually sent to other people, social media sites/apps or websites.
    - Phone call e.g. silent calls or abusive messages. The bully often disguises their number.
    - Email e.g. emailing upsetting messages, often using a different name for anonymity or using someone else's name to deflect the blame on them.
    - Chat room e.g. sending upsetting responses to people when they are in a web-based chat room.
    - Instant Messaging (IM) e.g. sending unpleasant messages in real-time conversations online.
    - Websites e.g. insulting blogs, personal websites, social networking sites and online personal polling sites.

22. Where conduct is found to be unacceptable, the College will deal with the matter internally and refer to relevant policies such as the staff and student code of conduct and disciplinary procedures. Where conduct is considered illegal, the college will report the matter to the police.

Online Communication

23. The bullet points below offer some guidance for both students and staff in their online communications:

- Do not create, store, exchange, display, print or circulate any message or media which may cause offense to others.
- Do not post or circulate any message which may be considered harassment
- Do not send messages at random or excessively, also referred to as "spamming", consider carefully the reply all function in email.
- Staff should not use personal social media accounts as a method of communicating with students.
- Staff should not give personal contact details to students.
- Student contact details must never be stored on a staff members' personal device(s), including computers, laptops, mobile phones, tablets, personal cloud or personal storage devices.
- College devices may, on occasion, be used to gather either video or photographic evidence in order to support students' course requirements provided that the college hold a signed authorisation form for the student in question.
- Do not give out log on details and passwords to anyone, the college will never ask you to disclose your password.
- Do not open files or emails from people you do not know. They may contain viruses or offensive material.
- If you see something abusive or upsetting online, you report it to a member of staff and/or the safeguarding team.
- Do not save your log-on details on shared computers as some people may use your name to cause harm to others.
- Make sure that your computer is locked when not in use so that others cannot act inappropriately using your profile.
- Do not post any confidential information to any online platform.
- Students should not send friend requests to members of staff, they are unable to accept them. Similarly staff should not seek to add students as friends on their personal social media accounts. Social media presences established in the interests of teaching and learning must be established in line with the college's social media policy.

Feedback and review

24. Staff and students are actively encouraged to review and feedback on this policy document. This is a working document and as such changes can be made throughout the year, the policy will be next formally reviewed and re-approved in 2024.