



Online Safety Policy 2026/27

Contents

1.Policy Statement	2
2.Scope	5
3.Introduction and purpose of the policy	5
4.College Values	6
5.Behaviour	6
6.College IT security	6
7.Responsibilities	7
8.Use of Images and Video	7
9.Student development	8
10.Staff development.....	8
11.Non – compliance	8
11.Report and support.....	8
12.Related Policies and Procedures	9
13. Location and access to the policy	9
14.Policy status and version control	9

If you have any queries around the content provided within this policy Or If you require this policy document in an alternative format, please contact: safeguarding@tameside.ac.uk

1. Policy Statement

1.1 Tameside College (Including Clarendon Sixth Form) is committed to promoting the safeguarding and welfare of students. This policy has been developed in line with DFE guidance: the latest Keeping children safe in Education and college's safeguarding policy.

1.2 At the core of our Online Safety Policy is a firm commitment to fostering equality, diversity and inclusion in full accordance with the [Equality Act 2010](#). We are dedicated to eliminating discrimination, advancing equal opportunities, and fostering an inclusive environment for all members of our college community. This commitment extends to every aspect of our processes, ensuring that it adheres to the legal obligations outlined in the [Equality Act 2010](#).

1.3 The College recognises the significant opportunities that digital technologies, including Artificial Intelligence (AI), provide to enhance teaching, learning and professional practice. We encourage students and staff to use technology to develop skills, improve achievement, promote creativity, increase accessibility and support lifelong learning. As digital technologies and AI become increasingly embedded in education, employment and everyday life, they also present ethical, academic, safeguarding and wellbeing challenges, including risks relating to accuracy, bias, privacy, misinformation and academic integrity and safety. The College is committed to promoting the safe, responsible and ethical use of technology by equipping students and staff with the knowledge, skills and critical understanding needed to navigate the online world confidently, respectfully and securely. Our aim is to prepare learners to use digital technologies and AI responsibly and professionally throughout their education, future employment and everyday lives.

1.4. Areas of risk for our college community include the following:

1.4.1 Content

- Exposure to inaccurate, misleading, biased, deceptive or harmful AI-generated content, information, advice and recommendations, including misinformation and content that may negatively affect decision-making, learning, safety or wellbeing.
- Exposure to age-inappropriate, distressing or harmful material that is unsuitable for young people or may negatively impact their health and wellbeing.

- Exposure to inaccurate, misleading or unreliable information online or generated through AI systems, without appropriate critical evaluation or verification.
- Exposure to socially unacceptable, harmful or extremist material, including content that promotes violence, hatred, discrimination, intolerance, radicalisation, self-harm or pornography.
- Exposure to illegal or criminal content, including child sexual abuse material, content promoting illegal activities, or material that breaches safeguarding requirements and legal obligations.
- Illegal downloading, sharing or distribution of copyrighted or protected materials, including music, films, software, images and other digital content.
- Exposure to AI-generated content that impersonates individuals, manipulates images, audio or video, or contributes to cyberbullying, harassment, fraud or online harm.
- Inappropriate sharing of personal, sensitive or confidential information with AI tools or online platforms, potentially compromising privacy and data protection.
- Over-reliance on AI-generated outputs without appropriate judgement, verification or understanding of ethical and academic responsibilities.

1.4.2 Contact

- Online grooming, exploitation, manipulation or coercion through communication technologies, social media, gaming platforms or AI-enabled tools, potentially leading to sexual abuse, child sexual exploitation, radicalisation or other forms of harm.
- Contact with individuals using false, assumed or anonymous identities online, including through gaming platforms, social networks and online communities, which may increase the risk of deception, manipulation or exploitation.
- Cyberbullying, harassment, intimidation, threatening behaviour or harmful communication through websites, social media, messaging platforms, mobile phones or other digital technologies.
- Unwanted or inappropriate contact from others online, including attempts to gain trust, obtain personal information, influence behaviour or encourage unsafe actions.

- Contact with individuals or groups who may promote harmful behaviours, including extremism, violence, exploitation, discrimination or other forms of online harm.
- Use of digital communication tools, including AI-enabled platforms, to impersonate, deceive, manipulate or target individuals.
- Risks associated with sharing personal information or communicating with unknown individuals online, which may compromise privacy, safety, wellbeing or safeguarding.
- The impact of online interactions on digital identity and footprint, reputation and relationships, including the long-term consequences of communication and behaviour in digital spaces.

1.4.3 Commerce

- Exposure to inappropriate, misleading or targeted commercial advertising, including marketing practices that may exploit young people, influence behaviour or promote unsuitable products and services.
- Exposure to online gambling, gaming-related financial risks, gambling-style features (such as loot boxes) or other services that may encourage harmful spending behaviours.
- Exposure to commercial scams, phishing attempts, fraud, fake websites, misleading offers or other online activities designed to obtain personal, financial or sensitive information.
- Risks associated with unsafe online purchasing, including counterfeit goods, fraudulent sellers, insecure payment methods or failure to understand digital consumer rights.
- Misuse of personal information for commercial purposes, including the collection, tracking or profiling of young people's online activity by digital platforms and AI-enabled services.
- Financial exploitation through online platforms, including scams, manipulation, social engineering or pressure to make inappropriate purchases or financial decisions.
- Lack of awareness of the value and protection of personal data, digital identities and online transactions when using commercial websites, apps and services.

2. Scope

- 2.1 This policy applies to all members of the college community (including staff, students, volunteers, parents/carers, visitors, community users) who have access to and are users of college IT systems and resources, both in and out of college.
- 2.2 The Online Safety Policy applies to all use of the internet and forms of electronic communication such as email, mobile phones, social media, instant messaging and use of AI.
- 2.3 It applies to any device used to access college IT resources.
- 2.4 This policy works in partnership with the IT Acceptable Use Policy and they should be read alongside each other.

3. Introduction and purpose of the policy

- 3.1 Online safety refers to the act of staying safe online. This is also known as internet safety, e-safety and cyber safety. It includes all devices which have access to the internet such as PCs, laptops and smart phones. Being safe online refers to individuals protecting themselves and others from online risks.
- 3.2 This policy sets out the college's approach and measures to ensure that all members of the college community can work in an e-safe environment and that any online safety issue is detected and dealt with promptly.
- 3.3 The specific purpose of the policy is to: -
- Ensure we provide a safe online environment for our members to learn and work.
 - Have effective filtering and monitoring measures to safeguard learners and staff from potentially harmful and inappropriate online material.
 - Equip our students and staff with the knowledge they may require to make the best use of the internet, technology and AI in a safe and considered way.
 - Promote use of online safety and activities in line with college values and staff Code of Conduct.
 - Ensure there are arrangements in place to address concerns.
 - Ensure filtering and protection systems do not result in unreasonable restrictions that may impact teaching and learning.

4. College Values

4.1 The college's values underpin and reflect our behaviours and play a critical role in shaping our college's work and study environment including online. We promote safeguarding, support a positive learning experience for all and our values play a key part in the way we wish to achieve our ambitions.

4.1 The college values are:

- Excellence through learning
- It's my responsibility,
- Work together
- Act with integrity
- Value and respect each other



5. Behaviour

5.1 Tameside College expects all students and staff to behave in line with its values.

5.2 We expect all users of technologies to adhere to the standard of behaviour as set out in the IT Acceptable Use Policy. The College will not tolerate any abuse of IT systems.

5.3 Whether offline or online, communications by staff and students should be courteous and respectful at all times.

5.4 Any reported incident of breaches, bullying or harassment or other unacceptable conduct will be treated seriously and in line with the relevant college policies and procedures.

6. College IT security

6.1 IT security including providing a safe online environment for our members to learn and work is a vital element of network infrastructure. The College has robust systems in place to ensure the College network is safe and secure and provides an important layer of defence against a wide range of threats. Every effort will be made to keep security software up to date. Appropriate security measures will include the use of enhanced filtering and protection of firewalls, servers, routers, work stations to prevent accidental or malicious access of college systems and information.

6.2 Digital communications, including email and internet postings, over the College network, will be monitored in line with the IT Acceptable Use Policy.

7. Responsibilities

7.1 The Assistant Principal for Student Services and Inclusion and Head of IT are responsible for maintaining this policy along with:

7.1.1 All tutors, who are responsible for embedding online safety education and practice into their teaching programme.

7.1.2 All College Managers who are responsible for implementing good online safety practice and safeguards consistent with this policy in their area of responsibility.

7.1.3 The College Safeguarding Committee overseeing and reviewing online safety arrangements including receiving relevant reports.

7.1.4 All members of College staff being aware, staying alert and responding appropriately to any potential or actual online safety (e-Safety) issue.

7.1.5 All students and staff are responsible for upholding expected standards of behaviour

8. Use of Images and Video

8.1 The use of images, or photographs, is popular in teaching and learning and should be encouraged where there is no breach of copy right or other rights of another person (e.g. images rights or rights associated with personal data). This will include images downloaded from the internet and those belonging to staff or students.

8.2 All students and staff should have awareness of the risks when taking, downloading and posting images online and making them available to others.

8.3 There are particular risks where personal images of themselves or others are posted onto social networking sites, for example.

8.3 Tameside College teaching staff will provide information to students on the appropriate use of images. This includes photographs of students and staff as well as using third party images. Our aim is to reinforce good practice as well as offer further information for all users on how to keep their personal information safe.

8.5 No image /photograph can be copied, downloaded, shared or distributed online without permission from the owner.

8.6 Photographs of activities on the College premises should be considered carefully and have the consent of the Marketing department before being published. Approved photographs should not include names of individuals without consent.

8.7 AI will should be used responsibly and effectively in line with guidance provided to students and staff to promote good practice.

9. Student development

9.1 Through the tutorial and personal development activities, students will be offered online safety information and training to enable them develop the required knowledge and skills needed to recognise online risks and to keep themselves safe while working online.

9.2 They will also be made aware of the filtering and monitoring arrangements that are in place at college, which aims to eliminate students' exposure to risks. Students are also made aware of how to report issues and access to sources of support and guidance (see 11 below).

10. Staff development

10.1 All new staff will receive online safety training as part of their induction programme, ensuring that they fully understand the college's online safety policy and IT Acceptable Use Policies. Refresher updates /training will be provided regularly.

10.1 All staff will have access to the relevant policies and college guidance.

11. non – compliance

11.1 Non-compliance and breach of the online safety policy may lead to disciplinary action according to this policy, IT Acceptable Use Policy, Acceptable Behaviour Policy and staff code of conduct, which are available to on CollegelP.

12. Report and Support

12. 1 if a student wishes to report an incident, they can do so through our safeguarding policy. This includes reporting concerns directly to their tutor, college managers or to the college's Safeguarding team, safeguarding@tameside.ac.uk.

12. 2 where a member of staff wishes to report an incident unrelated to students, they must contact their line manager as soon as possible or contact the IT team.

12.2 Where an online safety incident is reported to the College (through the safeguarding reporting methods, IT reporting reports or picked up as part of the filtering and monitoring measures) this matter will be dealt with very seriously, investigated and addressed. The College will act immediately to prevent, as far as reasonably possible, any harm or further harm occurring.

12.3 The college may involve external agencies if any issue involves safeguarding or criminal activities.

12.4 Students can access support from the wellbeing and safeguarding team.

12. Related Policies and Procedures

- [Safeguarding Policy](#)
- [IT Acceptable Use Policy](#)
- [Prevent Policy](#)
- [Staff Code of Conduct](#)
- [Acceptable Behaviour Policy](#)
- [Harassment and Bullying Policy](#)

13. Location and access to the policy

The Online Safety Policy and supporting policies and other documents are available via SharePoint on the College network and through course handbooks and inductions for students:

14. Policy status and version control

Version Control			
Author:	Assistant Principal – Student Services and Inclusion	Approved by:	<i>Senior Leadership Team & Governing Body</i>
Date Approved:	August 2026	Next Review Date:	August 2027
Responsible for review:	Assistant Principal – Student Services and Inclusion	Version Number:	1.0
Version Amendments			
Date of Amendment:		Amendments:	
Date of Amendment:		Amendments:	