SCARBOROUGH UTC

Technical Excellence, Employable Graduates

Scarborough UTC
Social Media Policy

Last updated: December 2021

Contents:

Appendices

Statement of intent

Scarborough UTC understands that social media is a growing part of life outside of college. We have a responsibility to safeguard our students against potential dangers when accessing the internet at college, and to educate our students about how to protect themselves online when outside of college.

We are committed to:

- Encouraging the responsible use of social media by all staff, parents and students in support of the college's mission, values and objectives.
- Protecting our students from the dangers of social media.
- Preventing and avoiding damage to the reputation of the college through irresponsible use of social media.
- Protecting our staff from cyberbullying and potentially career damaging behaviour.

Arranging online safety meetings for parents.

Signed by:

Principal Date: 1/12/21

Chair of the Governing Board Date: 1/12/21

1. Legal framework

1.1. This policy has due regard to all relevant legislation and statutory guidance including, but not limited to, the following:

- DfE (2018) 'Data protection: a toolkit for schools'
- The UK General Data Protection Regulation (UK GDPR)
- The Data Protection Act 2018
- The Computer Misuse Act 1990, amended by the Police and Justice Act 2006
- The Freedom of Information Act 2000
- The Safeguarding Vulnerable Groups Act 2006
- Equality Act 2010

1.2. This policy operates in conjunction with the following college policies:

- Technology Acceptable Use Agreement – Staff
- Online Safety Policy
- Student Code of Conduct
- Complaints Procedures Policy
- Anti-bullying Policy
- Allegations of Abuse Against Staff Policy
- Photography Policy
- Social Media Policy
- Acceptable Use Agreement
- Staff Code of Conduct
- Student Confidentiality Policy
- Data and E-Security Breach Prevention and Management Plan
- Child Protection and Safeguarding Policy
- Disciplinary Policy and Procedures
- Conduct for Learning

2. Roles and responsibilities

2.1. The principal is responsible for:

- The overall implementation of this policy and ensuring that all staff, parents and students are aware of their responsibilities in relation to social media use.
- Promoting safer working practices and standards with regards to the use of social media.
- Establishing clear expectations of behaviour for social media use.
- Ensuring that this policy, as written, does not discriminate on any grounds, including against any of the protected characteristics, as outlined in the Equality Act 2010.
- In conjunction with the governing board, handling complaints regarding this policy and its provisions in line with the college's Complaints Procedures Policy.
- Implementing appropriate sanctions and disciplinary methods where there is a breach of this policy.
- Taking steps to minimise the amount of misplaced or malicious allegations in relation to social media use.
- Working alongside the online safety officer and data protection officer (DPO) to ensure appropriate security measures are implemented and compliance with UK GDPR.

2.2. The governing board is responsible for:

- Ensuring the DSL's remit covers online safety.
- Reviewing this policy on an annual basis.
- Ensuring their own knowledge of online safety issues is up-to-date.
- Ensuring all staff undergo safeguarding and child protection training, including online safety, at induction.

2.3. Staff members are responsible for:

- Adhering to the principles outlined in this policy and the Technology Acceptable Use Agreement – Staff.
- Ensuring students adhere to the principles outlined in this policy and that it is implemented fairly and consistently in the classroom.
- Reporting any social media misuse by staff, students or parents to the principal immediately.
- Attending any training on social media use offered by the college.

2.4. Parents are responsible for:

- Adhering to the principles outlined in this policy.
- Taking appropriate responsibility for their use of social media and the influence on their children at home.
- Promoting safe social media behaviour for both themselves and their children.
- Attending online safety meetings held by the college wherever possible.
- Not engaging in activities involving social media which might bring the college into disrepute.
- Not representing their personal views as those of the college on any social medium.
- Acting in the best interests of students when creating, participating in or contributing to social media sites.

2.5. Students are responsible for:

- Adhering to the principles outlined in this policy and the Student Code of Conduct.
- Ensuring they understand how to use social media appropriately and stay safe online.
- Seeking help from college staff if they are concerned about something they or a peer have experienced online.
- Reporting online safety incidents and concerns in line with the procedures within this policy.
- Demonstrating the same high standards of behaviour as expected within the college.

2.6. The business manager is responsible for:

- Monitoring and reviewing all college-run social media accounts.
- Vetting and approving individuals who wish to be ‘friends’ or ‘followers’ on the college’s social media platforms.
- Consulting with staff on the purpose of the social media account and the content published.
- Maintaining a log of inappropriate comments or abuse relating to the college.
- Handling inappropriate comments or abuse posted on the college’s social media accounts, or regarding the college.

- Creating a terms of use agreement, which all content published must be in accordance with.

- Ensuring that enough resources are provided to keep the content of the social media accounts up-to-date and relevant.

2.7. ICT technicians are responsible for:

- Providing technical support in the development and implementation of the college's social media accounts.

- Implementing appropriate security measures as directed by the principal.

- Ensuring that the college's filtering and monitoring systems are updated as appropriate.

3. Definitions

3.1. For the purpose of this policy, the college defines **"social media"** as any online platform that offers real-time interaction between the user and other individuals or groups including, but not limited to, the following:

- Blogs

- Online discussion forums, such as NetMums

- Collaborative spaces, such as Facebook

- Media-sharing devices, such as YouTube

- 'Micro-blogging' applications, such as Twitter

3.2. For the purpose of this policy, **"cyberbullying"** is defined as any social media or communication technology intentionally used to bully an individual or group, including the posting or sharing of messages, images or videos.

3.3. For the purpose of this policy, **"members of the college community"** are defined as any teacher, member of support staff, student, parent of a student, governor or ex-student.

4. Data protection principles

4.1. The college will obtain consent from students and parents at the beginning of each academic year using the Social media consent form, which will confirm whether or not consent is given for posting images and videos of a student on social media platforms. The consent will be valid for the entire academic year. Consent provided for the use of images and videos only applies to college accounts – staff, students and parents are not permitted to post any imagery or videos on personal accounts.

4.2. Where a student is assessed by the college to have the competence to understand what they are consenting to, the college will obtain consent directly from that student;

otherwise, consent is obtained from whoever holds parental responsibility for the student.

4.3. A record of consent is maintained throughout the academic year, which details the students for whom consent has been provided. The DPO is responsible for ensuring this consent record remains up-to-date.

4.4. Parents and students are able to withdraw or amend their consent at any time. To do so, parents and students must inform the college in writing. Where parents or students withdraw or amend their consent, it will not affect the processing of any images or videos prior to when consent was withdrawn or amended. Processing will cease in line with parents' and students' requirements following this. Wherever it is reasonably practicable to do so, the college will take measures to remove any posts before consent was withdrawn or amended, such as removing an image from a social media site.

4.5. Consent can be provided for certain principles only, for example only images of a student are permitted to be posted, and not videos. This will be made explicitly clear on the consent from provided. The college will only post images and videos of students for whom consent has been received.

4.6. Only college-owned devices will be used to take images and videos of the college community, which have been pre-approved by the online safety officer for use. Only appropriate images and videos of students will be posted in which they are suitably dressed, i.e. it would not be suitable to display an image of a student in swimwear.

4.7. When posting on social media, the college will use group or class images or videos with general labels, e.g. 'sports day'.

4.8. When posting images and videos of students, the college will apply data minimisation techniques, such as pseudonymisation (blurring a photograph), to reduce the risk of a student being identified. The college will not post students' personal details on social media platforms and students' full names will never be used alongside any videos or images in which they are present.

4.9. Before posting on social media, staff will:

- Refer to the consent record log to ensure consent has been received for that student and for the exact processing activities required.
- Ensure that there is no additional identifying information relating to a student.

4.10. Any breaches of the data protection principles will be handled in accordance with the college's Data and Cyber-security Breach Prevention and Management Plan.

5. Staff social media use

5.1. College accounts

5.2. The college's social media sites will only be created and monitored by the communications officer and other designated staff members. There will be a strong pedagogical or business reason for the creation of social media accounts on behalf of the college; official college profiles and accounts will not be created for trivial reasons.

5.3. A college social media account will be entirely separate from any personal social media accounts held by staff members and will be linked to an official college email account.

5.4. Consideration will be given to the following aspects:

- The purpose for using social media
- Whether the overall investment will achieve the pedagogical aim
- The level of interactive engagement with the site
- Whether students, staff, parents or members of the public will be able to contribute content to the account
- How much time and effort staff members are willing to commit to the proposed site
- A clear plan which outlines aspects such as how long the site will last
- How the success of the site will be evaluated

5.5. College social media passwords are kept in the Business Manager's – these are not shared with any unauthorised persons, including students, unless otherwise permitted by the principal. Staff will adhere to the data protection principles outlined in section 4 of this policy at all times.

5.6. Staff will ensure any posts are positive in nature and relevant to students, the work of staff, the college or any achievements. Staff will not post any content online which is damaging to the college or any of its staff or students.

5.7. All content expressed on college social media accounts will not breach copyright, data protection or freedom of information legislation.

5.8. Staff will ensure the principal has checked the content before anything is posted on social media. If staff wish for reminders to be posted for parents, e.g. returning slips for a college trip, staff will seek permission from the principal before anything is posted.

5.9. If inappropriate content is accessed online, a report form will be completed and passed on to the online safety officer. The online safety officer retains the right to monitor staff members' internet usage in line with the Data and Cyber-security Breach Prevention and Management Plan.

5.10. The college's social media accounts will comply with site rules at all times, particularly with regards to the minimum age limit for use of the site. It will be noted that each networking site has their own rules which must be followed – the communications officer will induct staff to each new social media platform, providing them with the relevant training and information.

5.11. **Personal accounts**

5.12. Staff members will not access social media platforms during lesson times, but they are permitted to use social media during break times. Staff will avoid using social media in front of students.

5.13. Staff members will not use any college-owned mobile devices to access personal accounts, unless it is beneficial to the material being taught prior permission will be sought from the principal. Staff are not permitted to use the college's WiFi network to access personal accounts, unless otherwise permitted by the principal, and once the online safety officer has ensured the necessary network security controls are applied.

5.14. Staff will not 'friend', 'follow' or otherwise contact students or parents through their personal social media accounts. If students or parents attempt to 'friend' or 'follow' a staff member, they will report this to the principal.

5.15. Staff members will not provide their home address, phone number, mobile number, social networking details or email addresses to students or parents – any contact with students or parents will be done through authorised college contact channels. Staff members will use their college email address for college business and personal email address for their private correspondence; the two should not be mixed.

5.16. Staff members will ensure the necessary privacy controls are applied to personal accounts and will avoid identifying themselves as an employee of the college on their personal social media accounts. Where staff members use social media in a personal capacity, they will ensure it is clear that views are personal and are not those of the college.

5.17. No staff member will post any content online that is damaging to the college or any of its staff or students. Staff members will not post any information which could identify a student, class or the college – this includes any images, videos and personal information. Staff will not take any posts, images or videos from social media that belong to the college for their own personal use. Staff members will not post anonymously or under an alias to evade the guidance given in this policy.

5.18. Breaches of this policy by members of staff will be taken seriously, and in the event of illegal, defamatory or discriminatory content, could lead to prosecution, disciplinary action or dismissal. Members of staff will be aware that if their out-of-work activity brings the college into disrepute, disciplinary action will be taken.

5.19. Attempts to bully, coerce or manipulate members of the college community via social media by members of staff will be dealt with as a disciplinary matter.

5.20. Social media will not be used as a platform to attack, insult, abuse or defame students, their family members, colleagues or other professionals.

5.21. Staff members' personal information will not be discussed on social media.

6. Parent social media use

6.1. Parents are able to comment on or respond to information shared via social media sites; however, parents should do so in a way which does not damage the reputation of the college.

6.2. Parents will be asked not to share any photos or personal details of students when commenting on college social media sites, nor post comments concerning other students or staff members, in accordance with the Social Media Code of Conduct for Parents.

6.3. Any parents that are seen to be breaching the guidance in this policy will be required to attend a meeting with the principal, and may have their ability to interact with the social media websites removed.

6.4. Breaches of this policy will be taken seriously, and in the event of illegal, defamatory or discriminatory content could lead to prosecution.

7. Student social media use

7.1. Students will not access social media during lesson time, unless it is part of a curriculum activity. Students are not permitted to use the college's WiFi network to access any social media platforms unless prior permission has been sought from the principal, and the online safety officer has ensured appropriate network security measures are applied.

7.2. Students will not attempt to 'friend', 'follow' or otherwise contact members of staff through their personal social media accounts. Students are only permitted to be affiliates of college social media accounts. Where a student or parent attempts to "friend" or 'follow' a staff member on their personal account, it will be reported to the principal.

7.3. Students will not post any content online which is damaging to the college or any of its staff or students. Students will not post anonymously or under an alias to evade the guidance given in this policy.

7.4. Students are instructed not to sign up to any social media sites that have an age restriction above the student's age.

7.5. If inappropriate content is accessed online on college premises, it will be reported to a teacher.

7.6. Breaches of this policy will be taken seriously, and in the event of illegal, defamatory or discriminatory content, could lead to exclusion.

8. Online safety

8.1. Any disclosures made by students to staff about online abuse, harassment or exploitation, whether they are the victim or disclosing on behalf of another child, will be handled in line with the Child Protection and Safeguarding Policy.

8.2. Concerns regarding a staff member's online behaviour will be reported to the principal, who will decide on the best course of action in line with the relevant policies, e.g. the Staff Code of Conduct, Allegations of Abuse Against Staff Policy, and Disciplinary Policy and Procedures. If the concern is about the principal, it will be reported to the chair of governors.

8.3. Concerns regarding a student's online behaviour will be reported to the DSL, who will investigate any concerns with relevant staff members, e.g. the principal and ICT technicians, and manage concerns in accordance with relevant policies depending on their nature, e.g. the Behavioural Policy and Child Protection and Safeguarding Policy.

8.4. Where there is a concern that illegal activity has taken place, the principal will contact the police. The college will avoid unnecessarily criminalising students, e.g. calling the police, where criminal behaviour is thought to be inadvertent and as a result of ignorance or normal developmental curiosity, e.g. a student has taken and distributed indecent imagery of themselves. The DSL will decide in which cases this response is appropriate and will manage such cases in line with the Child Protection and Safeguarding Policy.

9. Blocked content

9.1. In accordance with the college's Data and Cyber-security Breach Prevention and Management Plan, the online safety officer will install firewalls on the college's network to prevent access to certain websites. The following social media websites are not accessible on the college's network:

- Twitter
- Facebook
- Instagram

9.2. The online safety officer retains the right to monitor staff and student access to websites when using the college's network and on college-owned devices.

9.3. Attempts made to circumvent the network's firewalls will result in a ban from using college computing equipment, other than with close supervision.

9.4. Inappropriate content accessed on the college's computers will be reported to the online safety officer so that the site can be blocked. Requests may be made to access erroneously blocked content by submitting a blocked content access form to the online safety officer, which will be approved by the principal.

10.Cyberbullying

10.1. Cyberbullying incidents are taken seriously at Scarborough UTC. Any reports of cyberbullying on social media platforms by students will be handled in accordance with the Anti-bullying Policy.

10.2. Cyberbullying against students or staff is not tolerated under any circumstances. Incidents of cyberbullying are dealt with quickly and effectively wherever they occur in line with the Anti-bullying Policy. Allegations of cyberbullying from staff members will be handled in accordance with the Allegations of Abuse Against Staff Policy.

11.Training

11.1. The college recognises that early intervention can protect students who may be at risk of cyberbullying or negative social media behaviour. As such, teachers will receive training in identifying potentially at-risk students. Teachers and support staff will receive training on social media as part of their new starter induction. Teachers and support staff will receive termly and ongoing training as part of their development.

11.2. Students will be educated about online safety and appropriate social media use on a termly basis through a variety of mediums, including assemblies, PSHE lessons and cross-curricular links. Students will be provided with material to reinforce their knowledge.

11.3. Parents will be invited to online safety and social media training on an annual basis and provided with relevant resources.

11.4. Training for all students, staff and parents will be refreshed in light of any significant incidents or changes.

12.Monitoring and review

12.1. This policy will be reviewed on an annual basis by the principal, in conjunction with the Business Manager and DPO.

12.2. The next scheduled review date for this policy is December 2022.

12.3. Any changes made to this policy will be communicated to all staff, students and parents.

Blocked content access request form

Requester	
Staff name:	
Date:	
Full URL:	
Site content:	
Reasons for access:	
Identified risks and control measures:	
Authoriser	
Approved?	✓ / X
Reasons:	
Staff name:	
Date:	
Signature:	

Inappropriate content report form

Staff name (submitting report):	
Name of individual accessing inappropriate content (if known):	
Date:	
Full URL(s):	
Nature of inappropriate content:	
To be completed by online safety officer	
Action taken:	
Staff name:	
Date:	
Signature:	

Social media consent form

This consent form provides information pertaining to how Scarborough UTC wishes to use personal data on social media, details the terms under which the college will use this data and requests consent for the college to use your personal data on social media.

Name of parent:	
Name of student:	
Year group:	

Why do we need your consent?

The college requests the consent of parents on an annual basis to use images and videos of their child for a variety of different purposes.

Without your consent, the college will not use images, videos, names or other forms of personal data of your child on social media. Similarly, if there are only certain conditions under which you would like images and videos of your child to be used, the college will abide by the conditions you outline in this form.

Why will we be using personal data on social media?

The college wants to use certain types of data on social media to promote the positive and inclusive ethos of the college – we aim to celebrate our students' and college's achievements and social media allows us to do this.

Where the college uses images of individual students, the name of the student **will not** be disclosed. Where an individual student is named in a written publication, a photograph of the student **will not** be used to accompany the text.

If, for example, a student has won an award and their parent would like their name to be published alongside their image, **separate consent** will be obtained prior to this.

With your consent, the college may use personal data on social media, the college website, in college prospectuses and other printed publications, such as a newsletter.

Who will be able to see the data once it's on social media?

The college's privacy settings only allow people who have been accepted to view the content on our social media platforms; additionally, where it is possible, the college's settings do not allow for further sharing. Please note, this sharing restriction may not be possible on all social media platforms, meaning that, if the content has been posted and is subsequently shared, more people will be able to view that piece of content.

What are the conditions of use?

- This consent form is valid for the current academic year.
- It is the responsibility of parents to inform the college, in writing, if consent needs to be withdrawn or amended.

- The college will not use the personal details or full names of any student in an image or video on social media.

- The college will not include personal emails, postal addresses, or telephone or fax numbers on images or videos on social media.

- The college may use pictures of students and teachers that have been drawn by students.

- The college may post pictures of work created by students on social media.

- The college may use group or class images or videos with general labels, e.g. 'sports day'.

- The college will only use images and videos of students who are suitably dressed, i.e. it would not be suitable to display an image of a student in swimwear.

- The college will not post any sensitive data, such as details of SEND, without express and additional consent, and will then still anonymise the posts.

Providing your consent

Please read the following conditions thoroughly and provide your consent as appropriate by ticking either 'Yes' or 'No' for each criteria.

The college will **only** post personal data on social media for the conditions that you provide consent for.

I provide consent to:	**Yes**	**No**
Using images of my child on the college's social media accounts.		
Using videos of my child on the college's social media accounts.		
Using images of my child on social media, including the following: **[Delete and/or add as appropriate]** • Twitter • Facebook • Instagram		
Using videos of my child on social media, including the following: **[Delete and/or add as appropriate]** • Twitter • Facebook • Instagram		

Using my child's first name on social media.		
Using my child's age on social media.		

Refreshing your consent

This form is valid for the entire academic year, it will be updated on an annual basis. Parents are required to fill in a new form for their child every academic year.

Consent will also be refreshed where any changes to circumstances occur – this can include, but is not limited to, the following:

- New requirements for consent, e.g. an additional social media account will be used to share student images and videos
- Changes to a student's circumstances, e.g. safeguarding requirements mean a student's image cannot be used
- Changes to parental consent, e.g. amending the provisions for which consent has been provided for

Where you would like to amend the provisions for which consent has been provided, you must submit your request in writing to the data protection officer (DPO). A new form will be supplied to you to amend your consent accordingly and provide a signature.

Withdrawing your consent

Parents have the right to withdraw their consent at any time. Withdrawing your consent will not affect the legality of processing personal data that was shared prior to withdrawal; however, the college will make every effort to remove posts about the student where possible, e.g. images of the student on social media will be removed.

If you would like to withdraw your consent, you must submit your request in writing to the DPO.

Declaration

I, ____________________ (name of parent), understand:

- Why my consent is required.
- The reasons why Scarborough UTC uses my child my child's personal data on social media.
- Who will be able to view my child's personal data once posted.
- The conditions under which the college uses personal data of my child on social media.
- I have provided my consent above as appropriate, and the college will act in accordance with my requirements.
- Consent is refreshed on an annual basis and I must re-provide consent in subsequent academic years.
- I will be required to re-provide consent where any circumstances change.

- I can amend or withdraw my consent at any time and must do so in writing to the DPO.

Name of parent: ______________________

Signature: ______________________

Date: ______________________

If you have any questions regarding this form, please do not hesitate to contact the DPO at vanessa.smallwood@scarboroughutc.co.uk or 01723 821 621.