

Social Media Policy

For the attention of: All Staff, Students, Governors, Contractors and Partners with access to Group-controlled accounts

Produced by: Group Exec Director Technology & Group Head of Marketing

Approved by: SLT

Date of publication: Date April 2026

Date of next review: Date July 2027





Vision, Purpose & Values

Our Vision

Our students will be recognised locally & nationally for their positive impact on the communities and industries in which they choose to work.

Our Purpose

To inspire our students to gain the skills, knowledge and behaviours they need to be resilient and thrive in an ever-changing world.

Our Values

Excellence: A culture of creativity, high expectations, ambition and aspiration

Respect: Showing fairness, courtesy and mutual respect to each other and our environment

Integrity: Honesty, openness and trust at the heart of College life

Diversity: Celebrating diversity and inclusivity as a key to our success

Contents

- Social Media Policy 1**
- Equality and Diversity 4**
 - 1. Purpose 4**
 - 2. Policy Statement 4**
 - 3. Policy Details 6**
 - 4. Online Safety Act 2023 14**
 - 5. Associated Documents 16**

Equality and Diversity

This policy is subject to the Equality Act 2010, which recognises the following nine Protected Characteristics under section 4 of the Act: age; disability; gender reassignment; marriage and civil partnership; pregnancy and maternity; race; religion or belief; sex; sexual orientation. The Group acts on socio-economic disadvantage as a positive-action priority under sections 158–159 of the Act, but socio-economic disadvantage is not a protected characteristic under the Equality Act 2010. Reasonable adjustments under section 20 of the Act are accommodated in the application of this policy. The Equality Act 2010 also gives rise to liability for harassment based on protected characteristics – a key cross-reference for section 3.3 (Keeping staff/students safe).

1. Purpose

- 1.1. This policy sets out the principles and rules which The Windsor Forest Colleges Group (TWFCG) staff (including, for the purposes of this policy, all TWFCG employees, temporary/ casual or agency workers, sessional staff, consultants or contractors engaged by TWFCG), Governors and students are required to follow when using internet-based social networking media. This includes Apps and websites such as Facebook, X, YouTube, Snapchat, Pinterest, TikTok, WhatsApp and LinkedIn, Bluesky, Instagram and any other social media sites, and also includes blog posts and personal websites. The term “social media” in this policy includes all such corporately maintained websites, blogs and personal websites.

2. Policy Statement

- 2.1. This policy does not form part of any contract of employment or contract for services and may be varied by TWFCG at any time.
- 2.2. Staff are encouraged to communicate with the student body through the TWFCG’s IT system, however, the TWFCG does allow staff and students to use social media, in accordance with this policy, to enhance and supplement their learning and overall college experience.
- 2.3. TWFCG actively uses social media – currently Facebook, X, Instagram, LinkedIn, TikTok, BlueSky & YouTube (but not limited to these) – to promote the College’s activities and to communicate with staff, students and the public.

- 2.4. When someone clearly identifies their association with TWFCG and/or discusses their work, they are required to behave professionally and respectfully when online and in ways that are consistent with the College's values and policies.
- 2.5. If you choose to have an online presence you must recognise that you are personally responsible for comments, photos, posts, videos, blogs, podcasts or any other content uploaded to a site, page or blog under your name, subject to the criminal-law and civil-law obligations summarised at section 4 of this policy.
- 2.6. This policy should be read in conjunction with TWFCG's other IT policies, safeguarding policies, disciplinary policy, student management policies, equality, diversity and inclusivity policy and data protection policy – in particular the Online Safety Policy, the AI Staff Policy, the UK GDPR Policy, the Privacy and Cookies Policy, the Group Safeguarding Policy and the Wearable Technology Policy. Your use of social media must also comply with all of TWFCG's other rules and policies including but not limited to those listed above.

2.7. **Photography**

In order to comply with data protection regulations, students are asked to provide their permission for photography at enrolment, as an additional precaution at general college events consent should be secured. When in a group situation students should be asked to give their verbal permission for their image to be used on social media and in college publicity. When an individual is photographed, they should sign a Photography Consent Form, this form should be sent to Marketing where it will be scanned and stored securely.

It is taken that Staff provide their consent for their images, presentations or videos to be used on the college social media sites. Any images or video taken are the property of the College and can be used freely, however students and staff have the right to refute their permission, at which time the College should remove the images from use wherever possible and should advise the person accordingly.

If an image is selected to be used more prominently in a campaign for both staff and students (i.e. on the cover of the guide or on campaign promotions), it is practice to secure a second level of consent for this more prominent use.

Staff should not post images of students on their personal social media accounts. If they have images of learners or staff participating in learning activities these should only be shared on approved WFCG social media

accounts via Marketing (except in regards to LinkedIn – please refer to the section below relating to LinkedIn).

3. Policy Details

3.1. Conduct rules

Staff and students who identify themselves as part of TWFCG:

- must not engage in activities online which might bring themselves or TWFCG into disrepute;
- must not use the internet in any way to attack or abuse students, staff or members of the public;
- must not post derogatory or offensive comments (whether or not directly related to TWFCG, colleagues, fellow students or themselves) which reflect poorly on TWFCG;
- must not make false or misleading statements – and must be aware that the false communications offence under s.179 Online Safety Act 2023 (in force 31 January 2024) criminalises sending a message containing information the sender knows to be false, with intent to cause non-trivial psychological or physical harm to a likely audience, without reasonable excuse (see section 4)
- must not impersonate colleagues, students or third parties or report anything on their behalf without their express agreement;
- may not use TWFCG logos and trademarks without the written consent of the Marketing department;
- must not engage in online with current or past students under any circumstance (except in regards to LinkedIn – please refer to section below relating to LinkedIn);
- must not (with explicit exceptions) use services such as WhatsApp, Telegram or other messaging Apps to create private groups for the purposes of discussing College activities, students or other staff members. TWFCG provides Microsoft Teams for creating work related group chats.
- Explicit exceptions to messaging groups, apply to 'Emergency comms' groups purposefully established outside of College systems for the purposes of communications in a lockdown or data breach scenario. These groups are

maintained by members of the senior leadership team, and provide access to key external partners.

- 'WhatsApp Business' groups including staff and students are only permitted on College owned devices for the sole purpose of communication during Trips & Visits, where setup in conjunction with IT Services, alternative methods of Communication are preferred. Staff are not permitted to use their personal WhatsApp in this scenario.
- The only exception is the use of WhatsApp Emergency Comms groups, these are setup and managed by the Group Executive Director Technology for the explicit purpose of managing business continuity, and are subject to audit and review. Members include Exec, SLT and selected Curriculum Leaders.
- Must refer any press enquiries, as a result of social media activities, to the Group Head of Marketing unless prior consent is given by Marketing or SLT.

3.2. **Reputation**

TWFCG is a further education College with children and young people under our care. As such standards of behaviour required of our staff are higher than one might expect in a typical corporate environment.

Maintaining the reputation of the College is vital – we pride ourselves on being an inclusive, respectful, tolerant, successful, exciting and vibrant place. Our online audiences must be confident in our brand and the integrity of the College as a whole. Therefore, it is crucial that contributions to social media from staff and students enhance and certainly do not undermine the College's reputation and ethos.

Staff and students must carefully think about their posts on social media sites that may affect the reputation of the College. For example, consider the content of photos that are uploaded after social events which may not present a professional image, consider the content of photos uploaded when the subject is wearing TWFCG branded clothing, and ensure that bad language and inappropriate behaviour is not used in posts. Staff and students must ensure that the content of their social media pages (including their profile) is consistent with the professional image which they present to colleagues and students. As a general guide staff and students should consider whether they would say in person what they intend to post to a student/parent or a tutor respectively. If doing so would be embarrassing for the member of staff or student or the person they are talking to, it is a good indication that the contents of the

proposed post are inappropriate and should not be posted. If you are unsure, do not post without seeking advice.

Remember that while it takes a matter of seconds to post something to a social media site, such posts can damage the College's or the member of staff's/student's reputation in a manner which can last for months if not years.

When a staff member or student is contacted by the press about posts on their social media page that relates to the College, the Group Head of Marketing must be consulted.

3.3. Keeping staff/students safe and appropriate behaviour

Staff and students should at all times take effective precautions when using social media to ensure their own personal safety.

Staff and students should always exercise caution when interacting with and responding to posts on social media sites that could be deemed as contentious.

Staff and students who use social media on campus must ensure that this usage complies with the College policies of acceptable use of IT and is used only when permitted by line managers and tutors respectively.

Social networking websites allow photographs, videos, personal details and comments to be shared with thousands of users. However, it may not be appropriate to share college-related information in this way.

Staff and students must not disclose confidential information about the College (including, but not limited to, financial aspects of the College and inspection reports) or students and/or their families or personal data about others via social media.

Staff and students should be considerate to their colleagues/peers and should not post information that is harassing, discriminatory, offensive, upsetting or inappropriate (particularly in the case of staff, bearing in mind their role is setting an example to students) or that they have been asked not to.

Under no circumstances should offensive comments be made about TWFCG, staff or students. This may amount to cyber-bullying and is likely to result in disciplinary action up to and including summary dismissal for staff and permanent exclusion for students. Conduct of this kind may also engage the criminal law: in particular, the false communications offence (s.179 Online Safety Act 2023, in force 31 January 2024); the threatening communications offence

(s.181 Online Safety Act 2023); the cyberflashing offence (s.184 Online Safety Act 2023, inserting s.66A Sexual Offences Act 2003); harassment under the Protection from Harassment Act 1997; sending grossly offensive, indecent, obscene or menacing messages under the Malicious Communications Act 1988; and harassment based on a protected characteristic under the Equality Act 2010.

Creating, sharing or threatening to share a sexually explicit photograph or film of any other person – including any image, whether or not a moving image, that has been altered by any means (capturing AI-generated and deepfake images of real persons) – without that person's consent is a criminal offence under section 66B of the Sexual Offences Act 2003 (as inserted by section 187 of the Online Safety Act 2023). This offence applies regardless of whether the image is shared on a public account or in a private group; it applies whether or not the subject ever existed in the depicted state; and it carries a custodial sentence on indictment.

Staff and students must uphold the College's value of respect for the individual and avoid making defamatory or negative statements about the College, its employees, its governors, its students, or their families.

Staff and students should also remove content immediately if asked to do so by a member of the management team or a tutor.

Staff and students should exercise care in setting appropriate boundaries between their personal and public online behaviour, understanding that what is initially private may easily become public in the digital world, even without their knowledge or consent. The College strongly encourages all staff and students to carefully review the privacy settings on any personal or College related social media and networking sites they use to ensure limited access to their personal information by people they are not "friends" with. Careful consideration should be given to accepting "friend"/"connection" requests – the College recommends particularly for students that they only accept "friend"/"connection" requests from people who they have actually met and know. The College encourages staff and students to exercise care and good judgment when posting content and information on such sites. Staff should appreciate that if they choose not to set privacy settings the contents of their social media pages will be accessible to all including current and prospective students and parents, colleagues and Governors, journalists and the press generally.

The Marketing department reserves the right to monitor the usage of all staff and students' social media sites and request the removal of content where the College considers that this is necessary or desirable.

In the event of an incident where a member of staff or student contravenes this policy, the member of staff/student may be subject to disciplinary action up to and including summary dismissal/exclusion. It is advised that any content posted publicly on social media can be used as evidence in instances of disciplinary action.

If a social media page makes it clear that the author works for or attends TWFCG, it must include a prominent, visible disclaimer explaining that the views on the page are personal and not those of the College such as:

"The comments and postings on this site are mine personally and should not be taken to reflect TWFCG's opinions, strategies or policies".

Staff: With particular reference to the College's Safeguarding Policy (incorporating Child Protection and Adults at Risk Procedures), staff are reminded that any form of personal relationship between staff and students who are under 18 years of age or are adult at risk (An adult at risk of abuse or neglect is defined as someone who has needs for care and support, who is experiencing, or at risk of, abuse or neglect and as a result of their care needs - is unable to protect themselves), is expressly forbidden. This would include any form of personal conversation or comment through the medium of the internet. As such, staff should not be 'friends' "followers," or any other similar terminology used by various sites with such students where information can be exchanged. The only platform where staff and student interaction is permitted is LinkedIn – please see below for more detail.

If staff/students are using social media in a personal capacity, use of this should be limited to lunchtimes or breaks but not during the working day/lesson times.

Staff and students should consider the timing of uploading content – content posted during the working/study day could be understood to refer to TWFCG even if express reference to TWFCG is not included in the content.

Staff and students must respect copyright laws and reference/cite sources appropriately. This also extends to accrediting photographers/videographers when their imagery is used. In this instance, permission must always be obtained prior to use.

If a member of staff or student thinks something on their social media page gives rise to concerns about a conflict of interest, and in particular concerns about impartiality or confidentiality, this must be discussed with their tutor/line manager and the Group Head of Marketing.

3.4. **Department use of Social Media sites**

If a staff member wishes to set up a social media platform for their subject area, they must seek written approval from the Group Head of Marketing in the first instance, and also allow the Marketing team full access and login details if the new platform is approved. Marketing has the right to disapprove any requests for departmental social media platforms if not deemed appropriate, or if it is felt that an additional social media presence would dilute our external presence. Marketing also reserves the right to close down any accounts not being used appropriately, or updated regularly.

If a student wishes to set up a social media platform for their College activities, then in the first instance the student should approach their tutor, who will in turn contact the Marketing department.

If a member of staff maintains or participates in a TWFCG-sponsored online community that extends to persons who are parents, alumni etc., they must exercise good judgment about any content that is shared on the site. This means that all content should reflect positively on TWFCG, its staff, governors and students.

3.5. **LinkedIn**

LinkedIn is a social networking site designed specifically for the business community. The goal of the site is to allow registered members to establish and document networks of people they know and trust professionally. A LinkedIn member's profile page, emphasises skills, employment history and education, has professional network news feeds and a limited number of customisable modules. Basic membership is free. Network members are called "connections". Unlike other free social networking sites, LinkedIn presumes 'connections' have a pre-existing relationship.

The College encourages the 'connection' between staff and learners providing the member of staff's own LinkedIn profile is completed to a suitable, professional standard. (If in doubt, please contact the Marketing department as training is available). Upon request, staff are permitted to 'Endorse' their learners for skills which they have gained on their study programme before they progress onto higher education or employment.

Under no circumstances is it acceptable to engage in Direct Messaging (DM) with students via LinkedIn, any and all communication via LinkedIn must remain transparent and publicly visible i.e comments on public posts.

It is acceptable to share images of the College Community on LinkedIn in circumstances where explicit permission is given by all parties, and official TWFCG accounts have been tagged for visibility. TWFCG and its community reserve the right to request that images are removed from LinkedIn.

When a staff member or student is contacted by the press about posts on their social media page that relates to the College, the Group Head of Marketing must be consulted.

3.6. **Confirmations**

a) Terms of use

By posting content on any social media page, you represent, warrant and agree that no content submitted, posted, transmitted or shared by you will infringe upon the rights of any third party, including copyright, trademark, privacy or contain defamatory, discriminatory or otherwise unlawful material.

b) User generated content disclaimer

You acknowledge that TWFCG accepts no responsibility or liability for any data, text, software, music, sound, photographs, images, video, messages or any other materials or content generated by users and publicity posted on any social media page under your name.

c) Disclaimer for content on linked sites

You acknowledge that TWFCG accepts no liability or responsibility whatsoever for the contents of any site linked from any social media page under your name.

3.7 **Synthetic media and deepfakes**

This sub-section is read alongside the Group's AI Staff Policy, which authorises a defined set of generative-AI image tools (Adobe Firefly, Canva, and the image-generation features of Microsoft Copilot and Google Gemini) for staff use, and the photography rules at section 2.7 above.

(a) AI-generated images of identifiable individuals. Generative-AI image tools can produce images that depict, or appear to depict, identifiable real persons.

Where an AI-generated image depicts an identifiable member of the Group community (staff, governor, student, parent or visitor), the same Photography Consent process at section 2.7 applies before the image is shared on any TWFCG-controlled or personal account: written consent from the individual depicted; written second-level consent for prominent campaign use; and Marketing's central record of consent.

(b) AI-generated images of under-18 students. AI-generated images depicting students under 18 must not be posted to any non-Group account. They may only be used on Group-controlled accounts where (i) the image is on the Group's MIS consent list, (ii) it has been routed through Marketing, and (iii) it has been reviewed by the Designated Safeguarding Lead chain where the image is at all ambiguous in respect of the student's safeguarding circumstances.

(c) Deepfakes — explicit prohibition. Creating, sharing, or threatening to share a synthetic or AI-altered image, video or audio clip that depicts any person in a sexual context without that person's explicit consent is a criminal offence under section 66B of the Sexual Offences Act 2003 (as inserted by section 187 of the Online Safety Act 2023). The offence applies whether the image was generated by a manipulating real source material ("face-swap"), generated wholly synthetically ("text-to-image"), or assembled by any combination. Any member of staff or student who creates or shares such content will be referred to the police in addition to disciplinary or exclusion action under this policy.

(d) Non-sexual deepfakes that may still cause harm. Deepfakes that fall outside section 66B but that depict identifiable individuals in misleading, defamatory or harassing ways may engage other criminal and civil liabilities — including the false communications offence (s.179 OSA 2023), the threatening communications offence (s.181 OSA 2023), harassment (PHA 1997), defamation (Defamation Act 2013), or harassment based on a protected characteristic (Equality Act 2010). Staff and students must not create or share such content on College-related accounts, and must be aware of the personal-liability exposure on personal accounts.

(e) Reporting. Suspected deepfake content depicting a member of the Group community — whether or not the suspected creator is connected to the Group — should be reported immediately to the Group Head of Marketing for take-down assessment, and to the DSL for safeguarding assessment. Where the content is sexual in nature or where the subject is under 18, the matter must be escalated to the police and to the Internet Watch Foundation (IWF) reporting portal.

4. Online Safety Act 2023

4.1. Scope and the Group's position

The Online Safety Act 2023 ("OSA 2023") is the principal UK statute regulating online safety. It creates two related sets of obligation that are relevant to this policy:

(a) Duties on providers of regulated user-to-user services and search services. These duties became operative on **17 March 2025** with the commencement of the OSA 2023 illegal-content duties for in-scope services, and have continued to expand under Ofcom's children's-safety regime through 2025–26. The Group is not itself a Category 1, 2A or 2B service and is therefore not subject to the provider duties. However, the Group's public-facing accounts on Facebook, X, Instagram, LinkedIn, TikTok, BlueSky, YouTube and equivalent platforms **interact with regulated services as a user**, which means that content originating on Group-controlled accounts is subject to those services' illegal-content and children's-safety controls. Marketing, working with the Group Head of IT and the DSL, is responsible for the College's posture as a user-of-services, including responding to take-down requests and to in-platform moderation actions.

(b) New criminal communications offences applicable to individuals. These offences came into force on **31 January 2024** and apply to staff, governors, students and contractors of the Group on the same basis as they apply to any individual in England and Wales. They are summarised at section 4.2.

4.2. Relevant criminal offences

The principal offences staff and students should be aware of are:

(a) False communications offence – section 179 OSA 2023 (replacing s.127(2) Communications Act 2003). It is an offence to send a message containing information the sender knows to be false, with the intention that it should cause non-trivial psychological or physical harm to a likely audience, without reasonable excuse.

(b) Threatening communications offence – section 181 OSA 2023. It is an offence to send a message conveying a threat of death or serious harm, intending or being reckless as to whether the recipient (or any member of an identifiable group of recipients) would fear that the threat would be carried out.

(c) Cyberflashing offence – section 184 OSA 2023, inserting section 66A into the Sexual Offences Act 2003. It is an offence intentionally to send or give a

photograph or film of any person's genitals to another person where (i) the sender intends the recipient to see the image and to cause alarm, distress or humiliation, or (ii) the sender sends it for the purpose of obtaining sexual gratification and is reckless as to whether the recipient is caused alarm, distress or humiliation.

(d) Sharing or threatening to share intimate images – section 66B Sexual Offences Act 2003 (as inserted by section 187 OSA 2023). It is an offence to share an intimate photograph or film of another person without that person's consent and without a reasonable belief in consent. The definition of "photograph or film" in section 66D SOA 2003 includes any image, whether or not a moving image, that has been **altered by any means** – which captures AI-generated and deepfake images of real persons. There are aggravated forms of the offence where the sharing is for the purpose of sexual gratification or to cause alarm, distress or humiliation.

(e) Encouraging or assisting serious self-harm – section 184 OSA 2023 (inserting offence into Serious Crime Act 2007). Staff and students should be alert to the offence and to the related safeguarding referral routes; suspected breach must be referred to the DSL chain immediately under the Group Safeguarding Policy.

Conduct that engages any of these offences is also, separately, a breach of this Social Media Policy and is liable to disciplinary action under section 3.3, irrespective of whether a criminal investigation is initiated.

4.3. **Children's safety and the Children's Code overlap**

Where Group-controlled social-media accounts are likely to be accessed by under-18 learners – which, given the Group's mission and audience, is the default case – the Group operates within the spirit of:

- Ofcom's Children's Safety Code under the OSA 2023 (commenced through 2025);
- the ICO's Age Appropriate Design Code (the "Children's Code"); and
- Keeping Children Safe in Education (KCSIE) 2025 (and the forthcoming KCSIE 2026 – consultation closed 22 April 2026, final text expected summer 2026 for commencement on 1 September 2026), in particular Part 2 on online safety.

Marketing-led content on Group-controlled accounts must not (i) link out to age-inappropriate material; (ii) embed third-party advertising or tracking that has not been assessed against the Children's Code; or (iii) use any feature that profiles or targets users under 18.

4.4. **Take-down and content moderation responsibilities**

(a) On Group-controlled accounts. The Group Head of Marketing is operationally responsible for moderation of Group-controlled accounts and for responding to take-down requests, in-platform reports, and Ofcom-consequent moderation actions. Where a take-down request relates to potentially illegal content (OSA 2023 s.179, 181, 184; SOA 2003 s.66A, s.66B), to safeguarding (DSL chain under the Group Safeguarding Policy), or to a personal-data matter (DPO under the UK GDPR Policy), Marketing must escalate immediately to the relevant lead and must preserve the content (and any platform metadata) for evidential purposes pending the decision.

(b) On personal accounts. Where staff, governor or student personal accounts post content that is alleged to engage any of the OSA 2023 / SOA 2003 offences and that affects the Group community, the College may (in addition to the disciplinary actions at section 3.3) request take-down by the relevant platform via the platform's reporting flow, and may report the matter to the police where the offence threshold is engaged.

(c) Records and evidence. Records of moderation decisions, take-down requests issued or received, and platform-side actions are retained per the Document Retention Policy and are accessible to the DPO on request.

4.5. **Cross-references**

This section is read alongside:

- the Group-wide Online Safety Policy
- the AI Staff Policy
- the Group Safeguarding Policy and KCSIE 2025 / 2026
- the UK GDPR Policy
- the Privacy and Cookies Policy
- the Wearable Technology Policy
- the IT Acceptable Usage Policy and its appendices

5. **Associated Documents**

- Online Safety Policy .
- AI Staff Policy .
- UK GDPR Policy .
- Privacy and Cookies Policy.
- Group Safeguarding Policy.

- Wearable Technology Policy.
- IT Acceptable Usage Policy and Appendices (Staff / Students / Temp).
- Document Retention Policy.
- Equality, Diversity and Inclusivity Policy.
- Disciplinary Policy; Student Behaviour and Discipline Policy.
- Photography Consent Form (Marketing).