



United Learning
The best in everyone™

Dunottar School

Social Media Policy

Contents

| | |
|---|----|
| Introduction | 3 |
| Key Personnel | 3 |
| Scope..... | 3 |
| Legal Framework..... | 4 |
| Professional Use of Social Media..... | 5 |
| Policy Statements | 6 |
| Names and Images..... | 6 |
| Safeguarding when taking Photographs..... | 7 |
| Parental Permission | 7 |
| Images of Pupils from other Schools | 8 |
| Images of Staff | 8 |
| Passwords and Account Security | 8 |
| Personal Use of Social Media | 9 |
| Policy Statements – Personal Use of Social Media..... | 9 |
| Social Networking Standards | 10 |
| Breaches of the policy..... | 12 |
| Document Information: | 13 |

Introduction

This policy has been drawn up with regard to relevant legislation and statutory guidance, including but not limited to:

- Keeping Children Safe in Education (KCSIE) (DfE), as amended from time to time.

This policy should be read alongside the School's Safeguarding and Child Protection Policy and Dunottar School IT Policies.

Social media and online platforms provide a range of tools that allow users to communicate, share information, and engage with wider communities. When used appropriately, these platforms can support positive communication and promote the work and values of the School.

This policy sets out the principles that all Dunottar School staff, volunteers, and contractors are expected to follow when using social media, whether in a professional or personal capacity where their role at the School may be identifiable.

It is essential that pupils, parents, and the wider public have confidence in the School's judgement, professionalism, and safeguarding practices. The principles within this policy are designed to ensure that social media is used responsibly, that the confidentiality of pupils and staff is protected, and that the reputation of Dunottar School and United Learning is upheld.

This policy also aims to support staff in using social media confidently and appropriately, while minimising professional risk. Staff must remain mindful of the need to maintain clear boundaries between their personal and professional lives at all times.

Key Personnel

Amanda Rowley (Marketing Manager) and Katie Tomlinson (Director of Admissions, Marketing and Communications) are responsible for creating and reviewing the policy.

While operational ownership of this policy sits with the Communications and Marketing Team, any safeguarding matters arising from social media use fall under the School's safeguarding framework and must be escalated to the Designated Safeguarding Lead (DSL) / Deputy Head (Pastoral) in line with the School's safeguarding procedures.

Scope

This policy applies to both the professional and personal use of social media by staff, volunteers, and contractors where their role at Dunottar School may be identifiable or where their online activity could reasonably be associated with the School.

It covers the use of social media and online platforms for official Dunottar School or United Learning purposes, including any accounts, pages, or content created, hosted, or maintained on behalf of the School or the Trust.

The policy applies to all forms of social media and online communication, including (but not limited to) social networking platforms, blogs, forums, messaging services, content-sharing platforms, and other publicly accessible online spaces.

The internet and digital technologies evolve rapidly, and it is not possible to anticipate every platform or form of online interaction. The principles set out in this policy therefore apply regardless of the platform or medium used.

Legal Framework

Dunottar School is committed to ensuring that all staff members handle information responsibly and provide services that meet the highest standards of confidentiality and professionalism. All individuals working on behalf of the School are bound by a legal duty to protect confidential and personal information accessed during the course of their work.

The inappropriate disclosure of information on social media, whether intentional or accidental, may constitute a breach of legal obligations and professional standards, including but not limited to:

- **The Human Rights Act 1998**, in particular Article 8 of the European Convention on Human Rights, which protects the right to respect for private and family life.
- **The common law duty of confidentiality**, which requires that information shared in confidence is not disclosed without a lawful basis, consent, or overriding public interest.
- **The UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018**, which together govern the processing, storage, sharing, and disclosure of personal data, including information relating to pupils, parents, staff, alumni, and third parties.

Staff should be aware that breaches of confidentiality or data protection law may result in disciplinary action and, in serious cases, legal or regulatory consequences. These duties apply equally to professional and personal use of social media.

Staff should also be aware of the guidance and sanctions contained within the Dunottar School Staff Handbook. Confidential information includes, but is not limited to:

- Person-identifiable information, e.g. pupil and employee records protected by the [Data Protection Act 2018](#) (see Data Protection Policy).
- Information divulged in the expectation of confidentiality.
- School or United Learning business or corporate records containing organisationally or publicly sensitive information.
- Any commercially sensitive information such as information relating to commercial proposals or current negotiations, and
- Politically sensitive information.

Staff should also be aware of the guidance, expectations, and potential sanctions set out in the Dunottar School Staff Handbook. Confidential information includes, but is not limited to:

- Personal data, including pupil, parent, and employee information, as defined and protected by the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (see the School's Data Protection Policy).
- Information disclosed in the expectation of confidentiality, whether explicitly stated or reasonably implied.
- School or United Learning business, governance, or corporate records containing organisationally sensitive or non-public information.

- Commercially sensitive information, including details relating to contracts, financial arrangements, commercial proposals, or ongoing negotiations.
- Politically or strategically sensitive information, including matters that could affect the School's reputation, governance, or relationships with regulators, partners, or the wider community.

Staff members should also be aware that other laws relating to defamation, harassment, communications, and intellectual property may apply to content posted on social media, whether in a professional or personal capacity. These include, but are not limited to:

- The Defamation Act 2013
- The Protection from Harassment Act 1997
- The Malicious Communications Act 1988
- The Communications Act 2003
- The Copyright, Designs and Patents Act 1988

Dunottar School and United Learning could be held vicariously responsible for acts of their employees in the course of their employment. For example, staff members who harass co-workers online or who engage in cyberbullying or discrimination on the grounds of race, sex, disability, etc. or who defame a third party while at work may render the schools and United Learning liable to the injured party.

Professional Use of Social Media

Many schools maintain a presence on social media platforms as an effective additional channel of communication with parents/carers, pupils, alumni, and the wider community. When used appropriately, social media can help celebrate achievements, share news, and promote engagement with school life.

Some staff may contribute to the School's professional use of social media, for example by sharing or supporting content that highlights successes, activities, or initiatives within their area of work, in line with School guidance.

However, the use of social media is not without risk, and staff members should be aware that:

- Social media platforms are public forums, routinely accessed by pupils, parents, journalists, employers, and the wider public.
- Content shared online may be copied, shared, or taken out of context, and should be considered permanent, even if later deleted.
- The School or United Learning may share or repost content originally published by staff members.
- Pupils or parents may share or comment on posts that relate directly to them, their family members, or their peers.

Staff should also be aware that some social media platforms allow anonymous or pseudonymous posting, which can increase the likelihood of offensive, misleading, or upsetting comments being directed towards schools or individuals.

New social media accounts must not be set up across any platform unless they are approved by the Communications and Marketing Team.

Policy Statements

Staff members should maintain a professional persona through any use of social media for work-related purposes. Usernames should be formal (e.g. @MrSmithSchoolName) or anonymised (e.g. @DunottarEnglish, @DunottarMaths). Anonymised accounts may also help to reduce the risk of online harassment. Staff are encouraged to submit all proposed content for social media to the Social Media Officer for posting via the School's official channels.

All professional content shared on social media must present Dunottar School and/or United Learning in a positive, professional manner. Posts should be written clearly and without ambiguity or rhetorical devices (such as sarcasm or irony), which may be misinterpreted in online contexts. Staff should remember that anything posted publicly may be shared widely and permanently and therefore represents the School. Care should be taken with spelling, grammar, punctuation, and tone.

School social media channels are used primarily as one-way communication tools for sharing information and celebrating school life. Staff must not enter into online dialogue with pupils via social media platforms. Limited professional interactions may take place with other schools or external organisations where appropriate (for example, acknowledging fixtures, visits, or collaborative events). Departmental accounts may also be used to share revision or study resources.

Pupils who follow departmental or school accounts should not be followed back, and their individual profiles should not be viewed or monitored by staff. Any attempt by pupils or other users to initiate direct interaction with staff through social media should be reported to the Deputy Head (Pastoral) for advice. In most cases, the appropriate response will be to address the matter offline. Staff should be aware that responding publicly to a pupil may confirm their status as a pupil at the School and link them to a wider digital footprint.

Where pupils interact with the School's official social media channels, including by commenting on or following accounts, this will be monitored by the Marketing Team. Any concerns relating to safeguarding or child protection will be escalated promptly to the Deputy Head (Pastoral) in line with the School's safeguarding procedures.

Staff are expected to exercise professional judgement at all times when using social media. Those who are new to social media are encouraged to seek advice from a senior colleague before posting. If there is any doubt about the appropriateness of content, the safest course of action is not to post it.

Appropriate disciplinary action may be taken where a member of staff makes a social media submission that brings Dunottar School or United Learning into disrepute.

Names and Images

Staff must take particular care when sharing names or images of pupils on social media.

Where a pupil is featured in a photograph, full names must not be used, and information that could identify the pupil further (such as form group or year group) must not be disclosed. In such cases, first names only may be used where appropriate. Posts that do not include an image of a pupil may include full names, but form groups should not be identified.

Images shared on social media should be selected carefully and must present the School positively. Images of pupils may only be published where appropriate consent has been obtained, in line with the School's data protection and safeguarding policies.

Staff should exercise caution when photographing pupils and must not upload images that could reasonably be considered embarrassing, intrusive, or inappropriate. Where possible, photographs of groups rather than individual pupils should be used, as this reduces focus on any one child and supports safeguarding best practice.

Safeguarding when taking Photographs

Staff must exercise particular vigilance when taking photographs of pupils for potential use on social media.

When taking photographs, staff must ensure that:

- Pupils are appropriately dressed, and where school uniform is worn, it complies fully with the School's uniform guidelines.
- Photographs of pupils in swimming costumes are not taken or used under any circumstances.
- Any visible name badges or identifying information are obscured or blurred before images are shared.

Images of pupils must only be taken and used where appropriate consent has been obtained, in line with the School's data protection and safeguarding policies.

Any safeguarding concerns arising from the use of social media, including unsuitable content, inappropriate communication, or online behaviour involving pupils, must be reported immediately to the Designated Safeguarding Lead (DSL) or Deputy Head (Pastoral), in accordance with the School's safeguarding procedures and statutory guidance set out in *Keeping Children Safe in Education (KCSIE)*.

To support safeguarding and professional accountability, staff must use school-issued equipment or approved school systems when taking photographs or recording images of pupils. Personal devices should not be used unless explicitly authorised by the School.

Parental Permission

Not all parents or carers have given consent for their child's image to be used on social media or other public-facing platforms. All staff involved in taking, submitting, or sharing photographs of pupils must be aware of these restrictions and ensure that such pupils are not included in images intended for publication.

Before taking or submitting photographs for social media use, staff must check the school's current record of pupils with limited or no photographic consent and take appropriate steps to avoid the inclusion of those pupils.

The register of pupils with restricted photographic permissions is available via the School's approved internal systems, and staff are expected to familiarise themselves with and follow this guidance at all times.

Failure to follow these procedures may place pupils at risk and may result in a breach of the school's data protection and safeguarding obligations.

Images of Pupils from other Schools

Where Dunottar pupils attend events alongside pupils from other schools, staff must exercise particular caution when taking photographs.

In most cases, it is not possible to be certain that parental consent has been given for pupils from other schools to be photographed. Any permission granted by parents is typically limited to the child's own school and does not extend to third parties. Staff must therefore assume that consent has not been given unless explicitly confirmed by the event organiser.

Staff must not authorise another school, organisation, or event organiser to take, share, or distribute images of pupils from other schools on Dunottar School's behalf.

At large public events where parents or carers are present (for example, sports fixtures with spectators or concerts with an audience), wide group shots may be acceptable. Even in these circumstances, staff should, where possible, focus images on Dunottar pupils.

At non-public events or smaller gatherings, staff must not take close-up photographs that clearly identify pupils from other schools. Instead, staff should seek alternative ways to record the occasion safely, such as:

- wide-angle photographs of a room or venue,
- images taken from behind or at a distance,
- photographs of Dunottar pupils arriving at, or preparing for, the event.

Images of Staff

Images of individual staff members must only be published or shared on social media where their explicit consent has been obtained. Images that could reasonably be considered embarrassing, intrusive, or inappropriate must not be published.

The same courtesy and standards apply to images of other adults, including visitors to the School and individuals encountered at external events, such as guest speakers, staff from other schools, visiting professionals, or event hosts.

Passwords and Account Security

Strong account security must be maintained for all school social media accounts to prevent unauthorised access, misuse, or reputational harm.

Staff responsible for managing or accessing school social media accounts must ensure that:

- Strong, unique passwords are used, incorporating a combination of upper- and lower-case letters, numbers, and symbols.
- Passwords used for school social media accounts are not reused for any personal or other professional accounts.
- Multi-factor authentication (MFA) is enabled wherever the platform allows.
- Passwords are stored securely and not shared with unauthorised individuals.

Devices used to access or post content to social media platforms must be password-protected or secured by biometric authentication to prevent third parties from posting on behalf of the School.

Unauthorised access to social media accounts — for example, where a third party posts content without the account holder’s knowledge or consent — can have serious and lasting consequences. School social media accounts may be deliberately targeted by pupils or others, and staff must remain vigilant at all times.

Any concerns about account security, suspected unauthorised access, or compromised passwords must be reported immediately to the appropriate senior member of staff in line with the School’s IT and data protection procedures.

Personal Use of Social Media

It is reasonable for staff to maintain personal online presences outside their professional role at Dunottar School. However, school staff occupy a position of particular trust due to their work with children and are expected to uphold high standards of professionalism and judgement at all times.

Staff should be mindful that content shared on personal social media accounts may have professional implications. Experience across the education sector has shown that poor judgement in the use of social media can have serious consequences for individuals and schools.

Staff are encouraged to consider carefully that information shared online, including text, images, and video:

- is rarely entirely private and can quickly enter the public domain.
- may be misinterpreted by audiences beyond its original intended context.
- may remain accessible for longer than intended.
- can be copied, shared, or reused by third parties without consent.

Staff should take steps to maintain clear boundaries between their personal online activity and their professional role. However, staff should also be aware that even where such boundaries are carefully managed, it may still be possible for pupils, parents, journalists, or others to link individuals to their professional role within the School.

For this reason, staff are expected to exercise sound professional judgement in all online activity and to ensure that their personal use of social media does not undermine confidence in their role, the School, or the wider school community.

Policy Statements – Personal Use of Social Media

With the exception of professional networking platforms such as LinkedIn, staff are advised not to identify themselves as employees of Dunottar School or United Learning within personal social media accounts, nor to present themselves as representing the views of the School or the Trust. This is intended to safeguard staff privacy and prevent personal content from being associated with the School. Staff must not use school logos, branding, or identifying details (including location) on personal accounts.

Staff must not have contact with pupils, or members of pupils’ families, via personal social media accounts, unless the pupil is a close family member. This includes accepting or initiating connections. Staff should be mindful that social media platforms often expose information through shared connections, even where direct contact has not been established.

Staff must decline any ‘friend’ or connection requests from pupils to personal social media accounts. Where appropriate, pupils may instead be signposted to the School’s official social media channels.

Staff must not initiate contact with former pupils via personal social media accounts while the former pupil is under the age of 18 or remains in full-time secondary or 16–19 education.

Staff should exercise caution when expressing political, religious, or philosophical views on personal social media. While staff are entitled to hold and express personal beliefs, content shared publicly must not undermine confidence in their professionalism or the School as a public-facing educational institution.

Staff must not use social media to document or distribute material relating to their private lives where this could reasonably bring the School or United Learning into disrepute, even where personal and professional accounts are kept separate.

Information accessed through employment, including personal or confidential information relating to pupils, families, colleagues, or other parties, must never be discussed or disclosed via personal social media accounts.

School email addresses or official contact details must not be used to create or manage personal social media accounts, or for communication via such platforms.

Staff should avoid editing publicly accessible online resources in a personal capacity while using school systems or networks, where this could be attributed to the School.

Caution is advised when connecting with colleagues on personal social media platforms, as these platforms may blur professional boundaries and affect working relationships.

Staff must not use social media or online platforms to attack, insult, harass, abuse, or defame pupils, their families, colleagues, other professionals, organisations, or the school.

Staff are strongly advised to ensure that privacy settings on personal social media accounts are set to the highest level available and to minimise public visibility wherever possible.

Any workplace concerns must be raised through the school's established internal procedures. Social media must not be used as a mechanism for raising concerns or grievances.

Social Networking Standards

The following standards apply to all employees of United Learning when using social networking and other online platforms.

DO:

- **Act responsibly at all times.** Even where you do not identify your profession or place of work, online conduct may still have professional implications and could jeopardise professional registration and/or employment.
- **Protect your privacy.** Consider carefully what information you share online and with whom. Use the highest available privacy settings and review them regularly. The more personal information that is shared, the greater the potential professional risk.
- **Manage online connections thoughtfully.** Restrict what information is visible to others and be selective about online connections.

- **Assume permanence.** Content shared online is rarely truly private. Even with strict privacy settings, information may be copied, redistributed, or taken out of context. Staff should assume that anything posted online may be permanent and widely shared.
- **Take appropriate action if subject to online abuse.** Where staff experience harassment, bullying, or abuse online, they should use platform tools to block or report inappropriate behaviour and seek support in line with the School's Safeguarding Policy.
- **Be considerate towards colleagues.** Images or information relating to colleagues must not be shared online without their consent. Any such content must be removed promptly if requested.
- **Respect the privacy of others.** Before sharing photographs or information from school or social events, consider whether those present would reasonably expect such material to appear on a public platform. Social media may not always be an appropriate forum for sharing information.
- **Act transparently when updating online information.** Where staff identify inaccurate or outdated information about the School online in the course of their work, any updates must be made transparently and with appropriate authorisation. Staff must consult their line manager before editing or amending information relating to Dunottar School.
- **Use social networking positively and professionally.** When used responsibly and with appropriate approval, social media can support professional development, communication, and networking. Any work-related blogs, accounts, or professional online activity must be discussed and agreed in advance with the relevant line manager.

DO NOT:

- Share confidential or personal information online. In line with the UK GDPR and the Data Protection Act 2018, staff must not share any identifiable information relating to pupils, their families, colleagues, or any other individuals. Confidential or sensitive information relating to Dunottar School or United Learning must not be disclosed online under any circumstances.
- Initiate, build, or pursue relationships via social media with pupils or members of pupils' families, whether current or former. If a connection request is received, this should be declined or ignored using platform tools. Any concerns about such contact should be discussed with a line manager.
- Use social media as a basis for professional decision-making or practice unless this forms part of an agreed role and has been explicitly approved by management in line with this policy.
- Discuss work-related matters online, including conversations about pupils, families, colleagues, internal issues, or any content that could identify the School. Attempts to anonymise such discussions do not make them appropriate.
- Post or share images of pupils or their families via personal social media accounts, even if requested to do so. Staff must not take photographs of pupils using personal devices in the workplace unless explicitly authorised and in line with School policy.
- Use social media to raise, escalate, or air workplace concerns. Any concerns must be raised through the School's established internal procedures, including discussions with a line manager or the appropriate policy for raising concerns.
- Engage in online activity that could reasonably bring the school or United Learning into disrepute, including behaviour, comments, or endorsements that undermine confidence in the School as a professional educational institution.
- Use social media as a forum for bullying, harassment, or abusive behaviour towards colleagues or others. Cyberbullying is addressed under the school's Bullying and Harassment Policy.
- Post, share, "like", or otherwise endorse derogatory, defamatory, or offensive content relating to pupils, their families, colleagues, the school, or United Learning.

All of the above standards apply equally to public and private areas of social media platforms where a staff member can be identified or associated with the school.

Breaches of the policy

Any breach of this policy may lead to disciplinary action being taken against the staff member involved in line with the United Learning Disciplinary Policy. A breach of this policy leading to breaches of confidentiality, defamation, or damage to the reputation of the School or United Learning or any illegal acts that render the School or United Learning liable to third parties will result in disciplinary action appropriate to the severity of the breach.

Where necessary, this could result in escalation to the Local Authority Designated Officer (LADO) and ultimately the Police. Contracted providers of services to the School/United Learning must inform the School/United Learning immediately of any breaches of this policy by their staff so that appropriate action can be taken to protect confidential information and limit the damage to the reputation of the School/United Learning. Any action against breaches should be according to contractors' internal disciplinary procedures.

Document Information:

| | | |
|---------------------------------|--|---|
| Name of Owner | John Weiner (owner from September 2023) M.Broughton | |
| Authorised by | M. Broughton | Oct 2016 |
| Date Document Reviewed | November 2016 | MB/ST |
| Reviewed and Updated | Aug 2017 | K.Lewis/ P.Crosthwaite/ M.Thomas/ S.Thorne |
| Policy updated | Jan 2018 | Change of Network Manager |
| Policy updated | April 2018 | Change of network manager |
| Next Review date | Aug 2018 | K.Lewis/ G. Wiles/ T.Stevens/ S.Thorne |
| Policy updated | Aug 2019 | Change of Social Media Officer |
| Policy updated | Apr 2020 | Addendum added for Covid-19 |
| Policy updated | Oct 2021 | K.Tomlinson |
| Policy updated | Oct 2022 | K.Tomlinson |
| Policy updated | Oct 2023 | K. Tomlinson |
| Policy updated | Oct 2024 | K. Tomlinson |
| Policy updated | April 2026 | K. Tomlinson |
| Governor responsible for Policy | Andy Porteous | |