Shoreham Academy

Social Media Policy

1st Edition. November 2016

Social Media Policy Shoreham Academy

2016

Contents Social Media Policy

Written by	*Mr T Harkins based on UL template*		*Business Director*	
Owned by	*Tim Harkins*		*Business Director*	
Applies to	Staff	Yes	Students	Yes
	Parents	Yes	Governors	Yes
Reviewed on	01/09/2016			
To be reviewed on	01/09/2017			
Version	1.0			

Key Personnel

Tim Harkins, Business Director; Martin Sacree, Vice Principal; Claire Perry, Director of Technology

Technical Expertise – Mr M Chapman, ICT Manager

Scope

This policy covers personal and professional use of social media as well as the use of social media for official United Learning/ academy purposes, including sites hosted and maintained on behalf of either.

This policy applies to personal web presences such as social networking sites (for example *Facebook*) blogs and microblogs (such as *Twitter)*, chatrooms, forums, podcasts, open access online encyclopaedias (such as *Wikipedia*), social bookmarking sites (such as *del.icio.us*) and content sharing sites (such as *flickr* and *YouTube*). The internet is a fast moving technology and it is impossible to cover all circumstances or emerging media - the principles set out in this policy must be followed irrespective of the medium.

Legal Framework

United Learning is committed to ensuring that all staff members provide confidential services that meet the highest standards. All individuals working on behalf of United Learning are bound by a legal duty of confidence and other laws to protect the confidential information they have access to during the course of their work. Disclosure of confidential information on social media is likely to be a breach of a number of laws and professional codes of conduct, including:

- the Human Rights Act 1998
- Common law duty of confidentiality, and
- the Data Protection Act 1998.

Staff should also be aware of the guidance and sanctions contained within the United Learning Disciplinary Policy

Confidential information includes, but is not limited to:

- Person-identifiable information, e.g. student and employee records protected by the Data Protection Act 1998 (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 members should also be aware that other laws relating to libel, defamation, harassment and copyright may apply to information posted on social media, including:

- Libel Act 1843
- Defamation Acts 1952 and 1996
- Protection from Harassment Act 1997
- Criminal Justice and Public Order Act 1994
- Malicious Communications Act 1998
- Communications Act 2003, and
- Copyright, Designs and Patents Act 1988.

Schools 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 and Academy Use of Social Media

The academy as with many other schools maintains a presence on various social media sites as they provide very effective additional channels of communication with parents/ carers, students and the wider community.

This is not without risk, however and staff members should be aware that;

- services such as Twitter are in the public domain and are regularly used by journalists, students, parents and employers
- submissions can take on a life of their own once sent by users, who should not rely on being able to delete them
- Schools and United Learning may re-tweet the submissions of staff members to their wider following
- Students or parents may retweet comments and pictures which directly relate to them, their family or their friends.

A picture of a girl with an outstanding piece of work is tweeted by the school – it does not name her – but is retweeted by the parent and mentions (@'s) his daughter. A predator would now have a picture, name and social media presence of parent and daughter. This may be enough to allow them to start grooming the individual.

- The ability to post anonymous comments to social media platforms, such as Twitter, may result in offensive or upsetting comments being directed at schools or staff.

Personal Use of Social Media

It is reasonable for members of staff to maintain personal web presences in their lives beyond their school life. Indeed, in 2012 over 53% of the UK population had a Facebook account.

School staff, however, occupy an almost unique professional position due to their work with children and the moral credibility they must maintain. There have been several recent cases where school staff have suffered serious professional consequences as a result of poor judgement in the use of social media.

It is worth considering that information (text, images, video) held in web presences;

- is never completely private and can very easily enter the public domain
- can be misinterpreted by audiences it was not originally intended for
- may persist beyond your wishes
- might be copied and used by third parties without your consent

It is therefore vital that use of social media in staff's lives beyond the school be totally separated from their professional identity. However, staff should be aware that even if this separation is strictly adhered to, it remains relatively easy for people (students, journalists, future employers etc.) to connect staff in schools with 'private' social media presences.

General social media use

- Expectations regarding safe and responsible use of social media will apply to all members of Shoreham Academy community and exist in order to safeguard both the academy and the wider community, on and offline. Examples of social media may include blogs, wikis, social networking, forums, bulletin boards, multiplayer online gaming, apps, video/photo sharing sites, chatrooms, instant messenger and many others.
- All members of the Shoreham Academy community will be encouraged to engage in social media in a positive, safe and responsible manner at all times.
- Information about safe and responsible use of social media will be communicated clearly and regularly to all members of the Shoreham Academy community.
- All members of the Shoreham Academy community are advised not to publish specific and detailed private thoughts, concerns, pictures or messages on any social media services, especially content that may be considered threatening, hurtful or defamatory to others.
- The academy will control students and staff access to social media and social networking sites whilst on site and using academy provided devices and systems.
- The use of social networking applications during school hours for personal use is/is not permitted.
- Inappropriate or excessive use of social media during school hours or whilst using academy devices may result in disciplinary or legal action and/or removal of Internet facilities.
- Any concerns regarding the online conduct of any member of the Shoreham Academy community on social media sites should be reported to the school leadership team and will be managed in accordance with existing school policies such as anti-bullying, allegations against staff, behaviour and safeguarding/child protection.
- Any breaches of academy policy may result in criminal, disciplinary or civil action being taken and this will depend upon the age of those involved and the circumstances of the wrong committed. Action taken will be in accordance with the relevant academy policies, such as anti-bullying, allegations against staff, behaviour and safeguarding/child protection.

Official use of social media

- Official use of social media sites by the academy will only take place with clear educational or community engagement objectives with specific intended outcomes e.g. increasing parental engagement.
- Official use of social media sites as communication tools will be risk assessed and formally approved by the principal.
- Official academy social media channels will be set up as distinct and dedicated social media site or account for educational or engagement purposes.
- Staff will use academy provided email addresses to register for and manage official school approved social media channels.
- Members of staff running official academy social media channels will sign a specific Acceptable Use Policy (AUP) to ensure they are aware of the required behaviours and expectations of use and to ensure that sites are used safely, responsibly and in accordance with local and national guidance and legislation.
- All communication on official academy social media platforms will be clear, transparent and open to scrutiny.

- Any online publication on official academy social media sites will comply with legal requirements including the Data Protection Act 1998, right to privacy conferred by the Human Rights Act 1998, or similar duty to protect private information and will not breach any common law duty of confidentiality, copyright etc.
- Official social media use by the academy will be in line with existing policies including anti-bullying and child protection.
- Images or videos of children will only be shared on official academy social media sites/channels in accordance with the academy image use policy.
- Information about safe and responsible use of academy social media channels will be communicated clearly and regularly to all members of the academy community.
- Official social media sites, blogs or wikis will be suitably protected (e.g. password protected) and where possible/appropriate, run and/or linked to from the academy website and take place with written approval from the Leadership Teams.
- Leadership staff must be aware of account information and relevant details for social media channels in case of emergency such as staff absence.
- Parents/Carers and pupils will be informed of any official academy social media use, along with expectations for safe use and academy action taken to safeguard the community.
- Shoreham Academy official social media channels are:
    - Twitter @Shoreham6form
    - Twitter @shorehamacademy
    - Twitter @shorehamPE
    - Full list - http://www.shoreham-academy.org/News-Events/Our-Twitter-Pages
    - Facebook https://www.facebook.com/Shoreham-Academy-Sixth-Form-906259942800610/
- Public communications on behalf of the school will, where possible, be read and agreed by at least one other colleague.
- The academy social media account will link back to the academy website and/or Acceptable Use Policy to demonstrate that the account is official.
- The academy will ensure that any official social media use does not exclude members of the community who are unable or unwilling to use social media channels.

Staff professional use of social media

- If members of staff are participating in online activity as part of their capacity as an employee of the academy, then they are requested to be professional at all times and that they are an ambassador for the school.
- Staff using social media professionally will disclose their official role/position but always make it clear that they do not necessarily speak on behalf of the academy.
- Staff using social media professionally will be responsible, credible, fair and honest at all times and consider how the information being published could be perceived or shared.
- Staff using social media officially will always act within the legal frameworks they would adhere to within the academy, including libel, defamation, confidentiality, copyright, data protection as well as equalities laws.
- Staff must ensure that any image posted on the academy social media channel have appropriate written parental consent.

- Staff using social media professionally will be accountable and must not disclose information, make commitments or engage in activities on behalf of the academy unless they are authorised to do so.
- Staff using social media professionally will inform their line manager, the academy online safety (e-Safety) lead and/or the principal of any concerns such as criticism or inappropriate content posted online.
- Staff will not engage with any direct or private messaging with students or parents/carers through social media and should communicate via academy communication channels.
- Staff using social media professionally will sign the academy social media Acceptable Use Policy before official social media use will take place.

Staff personal use of social media

- Staff members must not/are advised not to identify themselves as employees of the academy or United Learning in their personal web presences or purport to represent the views of either organisation
- Personal use of social networking, social media and personal publishing sites will be discussed with all members of staff as part of staff induction and will be revisited and communicated via regular staff training opportunities.
- Safe and professional behaviour will be outlined for all members of staff (including volunteers) as part of the school Acceptable Use Policy.
- All members of staff are advised not to communicate with or add as 'friends' any current or past pupils or current or past pupils' family members via any personal social media sites, applications or profiles. Any pre-existing relationships or exceptions that may compromise this will be discussed with line manager/ member of Leadership Team/principal.
- If ongoing contact with students is required once they have left the academy roll, then members of staff will be expected to use existing alumni networks or use official academy provided communication tools.
- All communication between staff and members of the academy community on academy business will take place via official approved communication channels (*such as school email address, Firefly VLE or school phone numbers*). Staff must not use personal accounts or information to make contact with students or parents, nor should any contact be accepted, except in circumstance whereby prior approval has been given by the principal.
- Any communication from students/parents received on personal social media accounts will be reported to the academy's designated safeguarding lead.
- Information staff members have access to as part of their employment, including photos and personal information about students and their family members, colleagues etc. will not be shared or discussed on personal social media sites.
- All members of staff are strongly advised to safeguard themselves and their privacy when using social media sites. This will include being aware of location sharing services, setting the privacy levels of their personal sites as strictly as they can, opting out of public listings on social networking sites, logging out of accounts after use and keeping passwords safe and confidential.
- All members of staff are encouraged to carefully consider the information, including text and images, they share and post online and should ensure that their social media use is

compatible with their professional role, in accordance with academy policies (safeguarding, confidentiality, data protection etc.) and the wider professional and legal framework.

- Members of staff will be encouraged to manage and control the content they share and post online. Advice will be provided to staff via staff training and by sharing appropriate guidance and resources on a regular basis.
- Members of staff will notify the Leadership Team immediately if they consider that any content shared or posted via any information and communications technology, including emails or social networking sites conflicts with their role in the academy.
- Staff members must not initiate contact with former students by means of personal social media sites whilst that pupil is under the age of 18 or in full time secondary or 16 to 19 education
- Staff members must not edit open access online encyclopaedias such as Wikipedia in a personal capacity from work
- Employees should be aware that United Learning has a policy for raising concerns at work and this should be followed should any concerns arise. Using a social networking site to raise any concerns at work will not be considered as appropriate
- Member of staff will ensure that they do not represent their personal views as that of the academy on social media.
- Academy email addresses will not be used for setting up personal social media accounts.
- Members of staff who follow/like the academy's social media channels will be advised to use dedicated professionals accounts where possible to avoid blurring professional boundaries.

Students use of social media

- Safe and responsible use of social media sites will be outlined for students and their parents as part of the school Acceptable Use Policy.
- Personal publishing on social media sites will be taught to students as part of an embedded and progressive education approach via age appropriate sites which have been risk assessed and approved as suitable for educational purposes.
- Students will be advised to consider the risks of sharing personal details of any kind on social media sites which may identify them and / or their location. Examples would include real/full name, address, mobile or landline phone numbers, school attended, Instant messenger contact details, email addresses, full names of friends/family, specific interests and clubs etc.
- Students will be advised not to meet any online friends without a parent/carer or other responsible adult's permission and only when they can be present.
- Students will be advised on appropriate security on social media sites and will be encouraged to use safe and passwords, deny access to unknown individuals and be supported in learning how to block and report unwanted communications.
- Students will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private/protected.
- Students will be informed of any official social media use with students and written parental consent will be obtained, as required.
- Any official social media activity involving students will be moderated by the academy where possible.

- The academy is aware that many popular social media sites state that they are not for children under the age of 13, therefore the Academy will not create accounts within school specifically for children under this age.
- Any concerns regarding students' use of social networking, social media and personal publishing sites, both at home and at school, will be dealt with in accordance with existing academy policies including anti-bullying and behaviour. Concerns will be raised with their parents/carers, particularly when concerning any underage use of social media sites.

Frequently Asked Questions

Why must staff members not upload video content to hosting services (such as YouTube) without sign off from the Director of ICT/Technology/ Principal. This is for reasons of safeguarding and for maintaining the reputation of the academy and United Learning. Likewise, staff members must not make use of any social media service with students apart from the academy's Learning Platform (Firefly) or The Hub, unless a pedagogical business case and associated risk assessment is agreed.

How can Staff members maintain a professional persona through any use of social media for work purposes? User names should be formal (e.g. @MrSmith_SchoolName) or anonymised (e.g. @PE_SchoolName). The latter option also distances the user from their real-life identify and makes online bullying less likely.

Why is it important not to use ambiguity or sarcasm? All professional submissions to social media sites must show the academy and/or United Learning in a positive light and should be written without ambiguity or any rhetorical device (such as sarcasm) which might be misinterpreted. It is surprisingly easy for even the gentlest of humour to be read differently than intended when parsed through abbreviated media such as Twitter.

Why must staff members not enter into dialogue using social media such as Twitter, which academies and United Learning are using purely as a one-way channel for distributing news. Any attempt by other users to interact with staff members via such services should be reported to the Director of ICT/ Principal/ appropriate delegated leader for advice and resolution. The simplest option is usually to take such issues offline. Even the simple act of responding to a student's tweeted question confirms that student attends the academy, links to their wider digital identity and photographs of them and does so in a purposefully public forum.

> *In asking questions of a teacher through Twitter the student identifies themselves as a student of that particular school, and expose their social media postings to the scrutiny of the wider community and possible bullying or exploitation. Students are encouraged to have private accounts but in order to receive a response from the teacher their account would need to be public.*

How to ensure you exercise professional judgement when using social media. If new to social media it is good practice to ask a senior colleague's opinion before posting an update to a social media service. If in doubt over the appropriateness of a submission, the best option is not to make it. Appropriate disciplinary action will be taken should a member of staff make a submission which brings the academy or United Learning into disrepute.

Any images submitted to a social media site should be chosen carefully and should show the academy positively. Look carefully at the work being shown; does it show good marking, are there spelling errors, are displays well laid out. When showing images of adults and children; are they dressed in line with the academy uniform policy, behaving appropriately?

Why must caution be used when uploading Images of students or staff?; Sometimes, close up images can identify the student and should be checked carefully. Likewise, no image which might reasonably be judged to cause embarrassment to the student should be published. 'Over the shoulder' images (where individuals are not recognisable) or group shots of 3 or more students are safest. Staff should seek advice from a senior colleague before publishing images of students wearing PE kit

Images of individual staff should only be uploaded with their consent and no image which might reasonably be judged to cause embarrassment to the member of staff should be published.

Individual staff may not want their digital image appearing online possibly because they have been subject of harassment in the past or are keen for ex-partners not to be able to find them. Although the image itself may not identify them additional information either on the academy website or how the image was subsequently reused may lead to distress.

Individual students should not be identifiable through submissions to social media sites, for safeguarding reasons. *For example, "Excellent piece of Level 7 work shown here by Tom in Y8" is acceptable, whereas including Tom's surname is not. Any submission that includes an image of a student must not make reference to the student's first, sur- or full name under any circumstances*.

However how other people retweet and reuse the image may lead to safeguarding issues as other followers mention the individual in the picture

How can I make sure I use a strong password security and prevent the social media account from being hi-jacked and misused? *Passwords should never be written down. A combination of upper and lower case characters should be combined with numerals. Passwords should be changed regularly and in line with school policy. The potential for hi-jacked accounts to bring schools and United Learning into disrepute is significant and responsibility for account security lies with the staff member who controls it. Staff should be cognisant that such accounts are likely to be targeted by pupils for precisely this purpose.*

Why is it important that devices used to post content to social media platforms should be password protected

Fraping (or Facebook raping) is where a third party changes a person's status or post inappropriate content to a social media platform without their consent or knowledge. The consequences can be long term and damaging.

A member of staff leaves their iPad in the classroom and is picked up by a student. Seeing he can access the staff member's twitter feed he proceeds to post racist comments. He is also able to change the password and email account associated with the twitter feed. He does not take the iPad. It takes 2 days for the member of staff to get the account deleted, during which time more comments have been added and seen by a significant number of parents, pupils and other professionals.

While out for an evening a friend picks up your phone and writes some "witty tweets" while you are at the bar. They do not reflect you as a member of staff and make people question your professional judgement. The same is possible on email and other communication platforms.

Why are we advised not to identify our employer on personal social media platforms? *This is to prevent information on these sites from being linked with the academy/ United Learning and to safeguard the privacy of staff members, particularly those involved in providing sensitive frontline services. Do not name the academy/ United Learning in any biographical detail associated with personal accounts or use their logos or any other identifying information (such as location).*

By adding school as an employer on Facebook it may be possible for people to search for all employees of the school at a future point, irrespective of your privacy settings.

Why can't I say what I like on my personal social media platform? Staff members should not put themselves in a position where extreme political, religious or philosophical views expressed via social

media conflict with those of a public institution such as a school. Even if separation of professional and private lives has been maintained, recent case history shows that teachers who express such views have found their position at school to be untenable. This information is now easier to find as it is possible to search Facebook for example, by likes, affiliation and places of employment. Likewise staff members should not use social media to document or distribute evidence of activities in their private lives that may bring the school or United Learning into disrepute.

Why should I not edit open access online encyclopaedias such as *Wikipedia* in a personal capacity from work? This is because the source of the edit will be recorded as the employer's IP address and the intervention will, therefore, appear as if it comes from the employer itself.

Social Networking Standards

Below sets out the standards expected of all United Learning employees when using social networking sites:

DO

- **Act responsibly at all times**. Even if you do not identify your profession or place of work, please be aware that your conduct online could jeopardise any professional registration and/or your employment.
- **Protect your own privacy**. Think through what kinds of information you want to share online and with whom you want to share this information. Adjust your privacy settings accordingly. Remember that the more personal information you share online, the more likely it is that something could have a negative impact on your employment. Think about managing your online friends by restricting what kind of information you give them access to.
- **Remember everything is public**. Even with the highest level of privacy settings, once something is online it can be copied and redistributed and it is easy to lose control of the information. Work on the assumption that everything you post on line will be permanent and will be shared with others.
- **Take appropriate action if you are the target of abuse online**. If you find yourself the target of bullying or abuse online then you can take action in dealing with this, such as blocking individuals from interacting with you and using the sites' support mechanisms to report inappropriate activity. The United Learning Bullying Action Policy also sets out support mechanisms to deal with cyber bullying issues.
- **Be considerate to your colleagues**. Pictures or information about colleagues should not be posted on social networking sites unless you have the agreement of the individual concerned. Always remove information about a colleague if they ask you to do so.
- **Respect the privacy of other**s. If photographs are taken at a United Learning event then check whether those in attendance expect that any photos may appear on a public social networking site before posting. Remember it may not always be an appropriate way to share information whether work related or not.
- **Update any online sources in a transparent manner**. In the course of work, employees may find errors or out of date information displayed through online encyclopaedias. If updating this information then you must be transparent about who you are and the capacity in which you are doing this. Employees should consult with their line manager before updating or amending any information about United Learning from an on line source.
- **Remember the benefits**. Used responsibly, social networking sites can be accessed to keep up to date with a number of professions and information. Many use Facebook, Twitter and LinkedIn to update and communicate with members. Work blogs may also be useful for communication, networking and professional development purposes but must be discussed and agreed with your relevant Manager/Group Leader.

DO NOT

- **Share confidential information online**. In line with the Data Protection Act 1998 employees should not share any child / young person / mother / father / carer identifiable information online or any personal information about colleagues. In addition to this, any confidential information about the United Learning should not be revealed online.
- **Build or pursue relationships with children, young people, mothers and fathers / carers**. Even if the child / young person / mother / father / carer is no longer within your care, United Learning does not deem this as appropriate behaviour. If you receive a request from a child / young person / mother / father / carer / then many sites allow you to ignore this request without the individual being informed to avoid any offence. If you are concerned about this in any circumstance, please discuss with your Line Manager.
- **Use social networking sites to inform professional practice**. There are some circumstances/ job roles where this may be appropriate however careful consideration and discussions with management should be applied in line with the information set out in section 5.5 of this policy.
- **Discuss work related issues online**. This takes into account conversations about child / young person / mother / father / carer / colleagues or anything else which may identify United Learning online and bring it into potential disrepute. Even if you think these conversations have been anonymised they are very likely to be deemed inappropriate.
- **Post pictures of children/young people/their mothers/fathers/carers**. Employees should take great care in posting any images of young people and/or their families. All posts should adhere to the academy Image Use policy
- **Raise concerns about your work**. Social networking sites should never be used for raising or escalating concerns at work. If you have concerns then these should be raised through either discussing with your line manager or following the United Learning's policy/procedure for raising concerns at work.
- **Engage in activities online which may bring the Organisation into disrepute**. Think through what activities you take part in whilst online and what you do or say that may bring United Learning into disrepute. Any reports of this will be reviewed in line with their appropriateness.
- **Be abusive to or bully other colleagues**. Social networking sites should not be used as a forum for abusive behaviour towards colleagues. *Cyber bullying and what it means is set out in our Bullying and E-Safety policies and procedures.*
- **Post derogatory, defamatory or offensive comments** about colleagues, the children / young person / mothers / fathers / carers, your work or Shoreham Academy. Everything posted on a social networking site should be deemed as open to the public and it is therefore unacceptable to use this as a forum for posting inappropriate comments.
- All of the above applies to both open and private sections of any social networking site with which employees identify themselves.