



## **Rationale**

The rise of increased access to global communication and the popularity of public social media networks poses potential risks for users given its unregulated nature. Leonardo da Vinci Academy recognises the opportunities presented by the use of public social media sites in an educational setting, but also seeks to protect school stakeholders from any potential issues that may arise.

## **Aim**

We aim to provide guidelines to protect all school stakeholders from any risk posed by public social media sites. Public social media networks are defined to include: Websites, blogs, wikis, online forums and virtual environments that fall outside of school regulated online pages (i.e. Facebook, Twitter, Myspace, TikTok, Instagram, Snapchat, Skype, LinkedIn, VK, etc...).

## **Implications**

### **Students**

- The school will provide 'public social media' safety classes as appropriate (incorporated into PSHE syllabus).
- Students should not use public social media in the school.
- Students should not seek to communicate with staff online, outside of school sanctioned systems.
- Students are advised to set the privacy settings of any social media sites they use to their highest available settings.
- Students are advised to think carefully about the content they post online; could the material posted be harmful or embarrassing in years to come?
- Students should be aware of 'cyber-bullying' and avoid situations that may hurt or harm themselves or others.

### **Staff**

- Staff should not access public social media sites from school networks unless for the purpose of school business and with permission of their line manager.
- Staff should not use their school issued email address for communication on public social networks that has not been approved by the school.
- Staff should not communicate online with students outside of school provided email addresses or systems.
- Staff should not 'friend', 'follow' or similar, students, nor provide personal email addresses unless the student is both over the age of 18, and no longer a member of this school.



- Staff should not make public postings or comments that may damage the reputation of the school, nor should they act as a spokesperson for the school unless granted permission by their line manager.
- Staff should not disclose on public social networks, any information that is confidential or proprietary to students, staff, parents or the school.
- Staff should not use the school's logo on any public social media networks without permission.
- Staff should not post photos of students on any public social media networks.
- Staff are advised to set the privacy settings of any public social media sites they use to the highest available settings. **See appendix 1 for specific advice regarding Facebook.**
- Staff are advised to remember that once posted online, material should be considered as forever available; think carefully about what you post online. Any communication received from children on any personal social media sites must be reported to the staff member's line manager. If any member of staff is aware of any inappropriate communications involving any child in any social media, these must immediately be reported as above.

Staff are advised not to accept or invite any ex-pupil of the school under the age of 18 as a friend, follower, subscriber or similar on any personal social media, or provide personal email addresses.

### Parents

Parents are advised to carefully monitor their child's public media usage and intervene as necessary.

### Non-Compliance

LEONARDO DA VINCI ACADEMY recognises the importance of the Social Media Policy and provides mechanisms for investigating and resolving non-compliance through the Anti-Bullying Policy, Behaviour Policy and School Regulations. All stakeholders should feel safe and secure in raising concerns with the appropriate member(s) of staff.

### To be read in conjunction with LEONARDO DA VINCI ACADEMY's:

- ICT Policy
- Anti-Bullying Policy
- Safeguarding Children Policy
- Staff Code of Conduct

Written by

Mr. Justin Kilcullen-Nichols on 1/1/22, Mrs. Vera Komarova



## Appendix 1: Facebook cheat sheet for staff

### Don't accept friend requests from pupils on social media

#### 10 rules for school staff on Facebook

1. Change your display name – use your first and middle name, use a maiden name, or put your surname backwards instead
2. Change your profile picture to something unidentifiable, or if not, ensure that the image is appropriate
3. Check your privacy settings regularly
4. Be careful about tagging other staff members in images or posts
5. Don't share anything publicly that you wouldn't be just as happy showing your pupils
6. Don't use social media sites during school hours
7. Don't make comments about your job, your colleagues, our school or your pupils online – once it's out there, it's out there
8. Don't associate yourself with the school on your profile (e.g. by setting it as your workplace, or by 'checking in' at a school event)
9. Don't link your work email address to your social media accounts. Anyone who has this address (or your personal email address/mobile number) is able to find you using this information
10. Consider uninstalling the Facebook app from your phone. The app recognises wifi connections and makes friend suggestions based on who else uses the same wifi connection (such as parents or pupils)

---

#### Check your privacy settings

- Change the visibility of your posts and photos to '**Friends only**', rather than 'Friends of friends'. Otherwise, pupils and their families may still be able to read your posts, see things you've shared and look at your pictures if they're friends with anybody on your contacts list
- Don't forget to check your **old posts and photos**
- The public may still be able to see posts you've '**liked**', even if your profile settings are private, because this depends on the privacy settings of the original poster
- **Google your name** to see what information about you is visible to the public
- Prevent search engines from indexing your profile so that people can't **search for you by name**
- Remember that **some information is always public**; your display name, profile picture, cover photo, user ID (in the URL for your profile), country, age range and gender



### What do to if...

#### A pupil adds you on social media

- In the first instance, ignore and delete the request. Block the pupil from viewing your profile
- Check your privacy settings again, and consider changing your display name or profile picture
- If the pupil asks you about the friend request in person, tell them that you're not allowed to accept friend requests from pupils and that if they persist, you'll have to notify senior leadership and/or their parents. If the pupil persists, take a screenshot of their request and any accompanying messages
- Notify the senior leadership team or the principal about what's happening

#### A parent adds you on social media

- It is at your discretion whether to respond. Bear in mind that:
  - Responding to one parent's friend request or message might set an unwelcome precedent for both you and other teachers at the school
  - Pupils may then have indirect access through their parent's account to anything you post, share, comment on or are tagged in
- If you wish to decline the offer or ignore the message, consider drafting a stock response to let the parent know that you're doing so

#### You're being harassed on social media, or somebody is spreading something offensive about you

- **Do not** retaliate or respond in any way
- Save evidence of any abuse by taking screenshots and recording the time and date it occurred
- Report the material to Facebook or the relevant social network and ask them to remove it
- If the perpetrator is a current pupil or staff member, our mediation and disciplinary procedures are usually sufficient to deal with online incidents
- If the perpetrator is a parent or other external adult, a senior member of staff should invite them to a meeting to address any reasonable concerns or complaints and/or request they remove the offending comments or material
- If the comments are racist, sexist, of a sexual nature or constitute a hate crime, you or a senior leader should consider contacting the police