ICT Acceptable Use Policy (AUP)
– Staff, Governors, Visitors and Students/Volunteers Agreement
2024/26

This policy document is adapted from Lancashire County Council's ICT AUP – Staff and was reviewed in August 2024

ICT and the related technologies such as e-mail, the Internet and mobile devices are an integral part of our daily life in school. This agreement is designed to ensure that all Staff, Governors, Visitors and Students/Volunteers are aware of their individual responsibilities when using technology, whether this is via personal devices or school devices, or on/off the school premises. All Staff, Governors, Visitors and Students/Volunteers are expected to sign this policy and adhere at all times to its contents. Any misuse of technology will not be taken lightly and will be reported to the head teacher for any necessary further action to be taken. Any concerns or clarification should be discussed with the Head teacher. Further guidance, details and clarification on specific points made in this agreement can be found in the school's Social Media and Mobile Phone Policies.

1. I will take responsibility for my own use of any technologies, making sure that I use them safely, responsibly and legally.

2. I will not use communications devices, whether school provided or personally owned, for bullying or harassment of others in any form.

3. I will not be involved with any online activities, either within or outside school that may bring the school, staff, children or wider community into disrepute. This includes derogatory/inflammatory comments made on social network Sites, forums and Chat Rooms.

4. I will not browse, download/upload or distribute any material that could be considered offensive, illegal or discriminatory. I will remain vigilant to ensure that children/adults are not accessing any materials that could incite extremism or radicalisation and report any concerns immediately to the head teacher.

5. I will respect copyright and intellectual property rights.

6. I will ensure that personal data (including data held on MIS systems) is kept secure at all times and is used appropriately in accordance with Data Protection legislation

7. I will ensure that images of pupils and/or adults will be taken, stored and used for professional purposes in line with school policy and with written consent of the parent/carer or relevant adult. I will not distribute images outside the school network without the prior permission of the parent/carer, or person/s in the image.

8. I will abide by the school's rules for using personal mobile equipment, including any handheld or wearable smart device, at all times.

9. I will report any known misuses of technology, including unacceptable behaviours of others, to the Head teacher or Online Safety Champion (Sam Stell).

10. I have a duty to report e-safety concerns in writing, or verbally, to the Head teacher or to our Online Safety Champion (Sam Stell).

11. I have a duty to respect the technical safeguards which are in place. I understand that attempting to breach technical safeguards or gain unauthorised access to systems and services is unacceptable.

12. I have a duty to protect passwords and personal network logins, and should lock my PC or log off the network when leaving workstations unattended. I understand that any attempts to access, corrupt or destroy other user's data, or compromise the privacy of others in any way, using any technology, is unacceptable.

13. I understand that network activities and online communications are monitored, including any personal and private communications made using school systems.

14. I will not install any hardware or software onto any school system.

15. I will only access the school's network using the safe remote access connection provided by BT Lancashire.

16. I understand that these rules are designed for the safety of all users and that if they are not followed, school sanctions will be applied and disciplinary action taken.
17. I will take care of all ICT equipment used and return it/store it safely in the designated place. I will report all faults in a timely manner to Sam Stell.

I have read and agree to follow this code of conduct and to support the safe use of ICT throughout the school.

Signature …… Date ……

Full Name Position/Role

…… (PRINT) ……

Safer Use of Social Networking and Social Media – Guidance for Staff, Governors, Visitors and Students/Volunteers

For the purpose of this guidance 'staff' is defined as:

- *any person employed by the school*
- *any person sitting on the governing body of the school*
- *any visitor to the school*
- *any student/volunteer undertaking a placement with the school*

Guidance for staff:

1. Consider how your online presence could possibly compromise your professional responsibilities. Think carefully before posting information, photographs or comments on the internet. Things that you might have thought funny at the time could potentially cause embarrassment to yourself or others. Online records are easy to create, but can be difficult, or in some cases, impossible to remove.

2. Exercise caution when divulging personal information online, for example your date of birth, home address etc. as this could potentially put you at risk of theft.

3. Do not give out your personal contact details to pupils – mobile number, email address etc.

4. Consider doing a Google search on yourself to check what information is held online about you. If any content is found that you would prefer not to be accessible, you can request that it is removed, by asking the person who uploaded it if you know them, or if appropriate, by using the 'report abuse' facility within the particular site.

5. Ensure you protect your social networking profile by utilising private settings so only friends can access and comment on your pages. However, be aware that your information could still appear on friend's pages, which may be publicly accessible.

6. Be aware that friends can tag you into photographs which you may not wish to be publicly available – ask people not to tag you without your consent. You can also untag yourself from Facebook photographs.

7. Maintain an appropriate distinction between your professional and personal life. Staff members who have an additional relationship with the school, for examples if their own children are pupils, or if they are active members of the community should not use online forums to raise any grievances they may have in relation to school.

8. Staff working in schools should never request/accept Facebook friend requests, or communicate online, with pupils, ex-pupils or parents. Check who is 'following' you on twitter and block pupils, ex-pupils and parents from receiving your updates.

9. Refrain from identifying your place of work, or making reference to the school on social networking sites.

10. Ensure you have a strong password for all social networking sites and that your electronic security is maintained by password protected equipment. Staff should never share passwords and log out of all computers fully after use. You should also ensure that school and personal property including mobile phones, laptops, i-Pads etc. are kept secure, so that children are not able to access them.

11. Never make, respond to, or take part in an online conversation that includes any offensive, abusive, derogatory, defamatory or inappropriate comments related to colleagues, pupils, parents or the school on the internet. Be conscious that information you disclose and opinions you express are in the public domain and as such, could potentially bring yourself and/or the school into disrepute.

12. Ensure that your own personal views cannot be misconstrued as you speaking on behalf of school. You can use statements such as "My view is…" or "In my opinion…"

13. Always comply with your school and professional body's codes of conduct, as well as policies/guidance on use of technology and the Safe Working Practices Guidance.

14. Never divulge any confidential information relating to school.

15. Do not use social networking sites for personal use during working hours.

16. Do not post any photographs or video footage taken at school onto websites without obtaining express written permission to do so.

17. In the event that you feel you have been a target of cyberbullying or inappropriate online behaviour, keep the evidence (screen prints, emails etc.) and report what has happened to your head teacher or a member of the leadership team. However, extreme caution must be exercised in relation to obscene material and staff members should not retain copies of information, but should instead report their concerns immediately to the head teacher for further investigation.

18. Overall, remember to be mindful of your professional responsibilities when using social media and be conscious that managing your online reputation is important for your current and future career. There is an increasing trend for employers to access social networking sites before interviewing job applicants so there is potential that your online activities could prevent you from progressing in your career. Equally, you could face disciplinary action if your employer feels that your use of social networking is inappropriate.