# SOCIAL NETWORKING POLICY & Acceptable Use Agreement

## NANCLEDRA SCHOOL

### February 2018

**Preamble**

The almost overwhelming tide of social networking sites has been described by ACAS as 'an HR accident waiting to happen'. We now know from experience that this is proving to be true and that employers are grappling with how to deal with employees who post malicious comments about an employer, colleague or student for the world to see.
Yet this has proved to be one of the more challenging changes in terms of controlling misuse by members of staff both in and outside school. Opinion is divided as to whether social media are a threat or an opportunity: on the plus side, they provide an interactive platform for marketing and getting up-to-the-minute information to a wide audience quickly and cost-effectively. On the downside, they pose a potential data security and 'school-into-disrepute' risk and the benefits described above can be counteracted by negative publicity getting into the public domain.

**Scope of the Policy**

This policy applies to all staff, volunteers and Governors representing the School. It aims to give advice and establish protocols for representatives of the school who use social media sites to ensure such activities are mindful of the reputation of the school, fellow professionals and colleagues working within the school and the individual's own professional standing. It pertains to using such media both inside and outside the school and principally when members use such media at home. The School Staffing Regulations 2009 place a duty on an employer of staff in schools (be that a maintained, Academy, Voluntary Aided, or Trust) to invoke the school's disciplinary procedure where acts of misconduct have occurred. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place off-site, but is linked to membership of the School.
The School will deal with such incidents within this policy and associated behaviour and anti-bullying policies (linked to the Whole School Disciplinary Policy and Grievance Policy)

**Governors**

Governors are responsible for the approval of this Policy and for reviewing its effectiveness. A member of the Governing Body has taken on the role of E-Safety Governor and will work via the Senior Leadership Team to ensure compliance with this policy.

# GUIDELINES FOR STAFF

**a) Use of social media both in and outside school**

It is recommended that staff should receive training in the correct use of social media in order to avoid instances of inappropriate behaviour or blurring of the boundaries of responsibilities when using such media. Cornwall Council is able to facilitate such training via Cornwall Learning Academy. The link to the Embracing Social Media one day course is www.cornwall.gov.uk/learningacademy.

When using communication technologies the following is considered as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Staff and students should therefore use only the school email service to communicate with others when in the school, or on the school systems (eg: by remote access).
- Users need to be aware that email communications may be monitored
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff and students or parents / carers (email, chat, VLE etc) must be professional in tone and content. These communications may only take place on official (monitored) systems. Personal email addresses, text messaging or public chat / social networking programmes must not be used for these communications.
- Both staff and students are taught about email/social network safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.
- Personal information should not be posted on the school's website and only official email addresses should be used to identify members of staff.

- **Use of social networking sites using school equipment is not allowed**.
- **The safeguards listed below must be followed.***
- **These same safeguards apply to members of the school community who access social media at home /outside the school**

* Guidance for Safer Working Practice for Adults who work with Children & Young People, DFES Publication, Jan 09, paragraph 13 . " "ensure that if a social networking site is used, details are not shared with children and young people and privacy settings are set at a maximum".

**i) Relationships and attitudes**

(a) All staff should clearly understand the need to maintain appropriate boundaries in their dealings with pupils.

(b) All staff should ensure that their electronic communications with pupils are appropriate to the age and gender of the pupils, and take care that their language or conduct does not give rise to comment or speculation. Attitudes and language all require care and thought, particularly when members of staff of either sex are dealing with adolescent boys and girls.

(c) From time to time staff may encounter pupils who display attention seeking behaviour, or profess to be attracted to them. Staff should aim to deal with those situations sensitively and appropriately, but must ensure that communications cannot be misinterpreted. In these circumstances, the member of staff should also ensure that the head teacher or a senior colleague is aware of the situation.

**ii) Inappropriate e-mail/social networking comments and discussions with pupils**

(a) Comments by staff to pupils, either individually or in groups, can be misconstrued. As a general principle therefore staff must not make unnecessary comments to and/or about pupils which could be construed to have a sexual connotation. It is also unacceptable for staff to introduce or to encourage debate amongst pupils which could be construed as having a sexual connotation.

(b) Systematic use of insensitive, disparaging or sarcastic comments are also unacceptable. These are clear examples of 'cyberbullying'.

**iii) Reporting incidents**

Following any incident where a member of staff feels that his/her electronic communications have been, or may be, misconstrued, he/she should discuss the matter with the Headteacher. Where it is agreed with the head teacher, the member of staff or volunteer should provide a written report of the incident.

**b) Advice with regard to Cyberbullying**

When publishing information about yourself or having conversations with others online, it is important to be mindful of how you present yourself, who can see your content, and how you can manage it appropriately. When publishing information on a social networking site (such as personal details, images) ask yourself if you would feel comfortable about a current or prospective employer, colleague, student or parent, viewing your content.

Make sure you understand who is allowed to view your content on the sites that you use and how to restrict access to your account. If you are not clear about how to

restrict access to your content, you must regard all the content as publicly available and therefore act accordingly.

Use search engines to check what images/text are associated with your name. This will help establish what information other people can find out about you.

Often, staff become aware of other people posting objectionable material about them from others. Encouraging everyone to report any incidents they find, rather than be a passive bystander, is an important strand of preventing cyberbullying.

If you have a social networking account, DO NOT befriend pupils or add them to your contact lists. In so doing you may be giving them access to personal information and allowing inappropriate contact.

Appendix 1

# Social Networking Policy Staff (and Volunteer) Acceptable Use Agreement

New technologies have become integral to the lives of children and young people in today's society, both within schools/academies and in their lives outside the Academy. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe internet access at all times.

This Acceptable Use Agreement is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that the School's ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of ICT in their everyday work and when using social networking sites both at work and at home

.

The School will try to ensure that staff and volunteers will have good access to ICT to enhance their work, to enhance learning opportunities for students learning and will, in return, expect staff and volunteers to agree to be responsible users.

# NANCLEDRA SCHOOL

**Acceptable Use Agreement**.

I understand that I must use the School ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that pupils receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed e-safety in my work with young people.

For my professional and personal safety:

• I understand that the School will monitor my use of the ICT systems, email and other digital communications.
• I understand that the rules set out in this agreement also apply to use of School ICT systems (eg laptops, email, website etc) outside the School
• I understand that the School ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the School.
• I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password.
• I will immediately report any illegal, inappropriate or harmful material or incident that I become aware of, to the appropriate person.

I will be professional in my communications and actions when using School ICT systems:

• I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
• I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the School's policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (eg on the School website) it will not be possible to identify by name, or other personal information, those who are featured. The School and (where necessary) the local authority have the responsibility to provide safe and secure access to technologies.

When I use my personal hand held / external devices (PDAs / laptops / mobile phones / USB devices etc) in the School, I will follow the rules set out in this agreement, in the same way as if I was using School equipment. I will also follow any additional rules set by the School about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.

• I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
• I will ensure that my data is regularly backed up, in accordance with relevant School policies.

• I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
• I will not disable or cause any damage to School equipment, or the equipment belonging to others.
• I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School/ LA Personal Data Policy. Where personal data is transferred outside the secure School network, it must be encrypted.
• I understand that data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by School policy to disclose such information to an appropriate authority.
• I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for School sanctioned personal use:

• I will ensure that I have permission to use the original work of others in my own work
• Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of school:

• I understand that this Acceptable Use Agreement applies not only to my work and use of ICT equipment in the School, but also applies to my use of School ICT systems and equipment out of School and my use of personal equipment in the School or in situations related to my employment by the School.

• I understand that if I fail to comply with this Acceptable Use Agreement, I could be subject to disciplinary action. This could be a warning, a suspension, referral to Governors and / or the Local Authority and in the event of illegal activities the involvement of the police.
• I have read and understand the above and agree to use the School ICT systems (both in and out of the School) and my own devices (in the School and when carrying out communications related to the School) within these guidelines.

Staff / Volunteer Name ……..

Signed……..

Date …….