Slyne-with-Hest C of E Primary School

POLICY ON THE USE OF SOCIAL NETWORKING SITES AND OTHER FORMS OF SOCIAL MEDIA including Staff Acceptable use agreement

(Initial policy Sept 2018 – amended and updated September 2021)

Policy:	Use of Social networking sites and AUP
This statement was approved:	November 2020
This statement will be reviewed:	Annually (Nov 2021)
Governor committee responsibility:	Full governing body

The Governing Body of Slyne-with-Hest St Luke's CEPS adopted the initial policy on 21/11/18. The policy will be reviewed on an annual basis. **Last reviewed November 2020 – additions made Sept 2021 to be agreed at November 2021 review.**

This Policy has been developed in consultation with the recognised Trade Unions and professional Associations.

1. **PURPOSE**

   This Policy sets out the school's position regarding the use of social networking sites and other forms of social media. The aim of the document is to ensure that all employees are fully aware of the risks associated with using such sites and their responsibilities with regards to the safeguarding and protection of both children and themselves.

2. **APPLICATION**

This Policy applies to all staff employed in delegated schools and those Teachers employed in Centrally Managed Services.

3. BACKGROUND

3.1 The use of social networking sites such as Facebook, Twitter, Pintrest, LinkedIn and MySpace has over recent years become the primary form of communication between friends and family. In addition there are many other sites which allow people to publish their own pictures, text and videos such as YouTube, Instagram and Snapchat.

3.2 It would not be reasonable to expect or instruct employees not to use these sites which, if used with caution, should have no impact whatsoever on their role in school. Indeed, appropriate use of some sites may also have professional benefits. For example many schools now use sites such as Facebook and Twitter as a means to enhance parental engagement.

3.3 It is now widely acknowledged that use of such sites does not provide a completely private platform for personal communications. Even when utilised sensibly and with caution employees are vulnerable to their personal details being exposed to a wider audience than they might otherwise have intended. One example of this is when photographs and comments are published by others without the employees consent or knowledge which may portray the employee in a manner which is not conducive to their role in school.

3.4 Difficulties arise when staff utilise these sites and they do not have the relevant knowledge or skills to ensure adequate security and privacy settings. In addition there are some cases when employees deliberately use these sites to communicate with and/or form inappropriate relationships with children and young people.

4. GUIDANCE AND ADVICE

4.1 Employees who choose to make use of social networking site/media should be advised as follows:-

(i) That they should not access these sites for personal use during working hours;

(ii) That they familiarise themselves with the site's 'privacy settings' in order to ensure that information is not automatically shared with a wider audience than intended;

(iii) That they do not conduct or portray themselves in a manner which may:-

- bring the school into disrepute;
- lead to valid parental complaints;
- be deemed as derogatory towards the school and/or it's employees;
- be deemed as derogatory towards pupils and/or parents and carers;
- bring into question their appropriateness to work with children and young people.

(iv) That they do not form on-line 'friendships' or enter into communication with *parents/carers and pupils as this could lead to professional relationships being compromised.

(v) On-line friendships and communication with former pupils should be strongly discouraged particularly if the pupils are under the age of 18 years.

(vi) That they could face legal proceedings if comments they post about named individuals are found to have harmed their reputation.

*(*In some cases employees in schools/services are related to parents/carers and/or pupils or may have formed on-line friendships with them prior to them becoming parents/carers and/or pupils of the school/service. In these cases employees should be advised that the nature of such relationships has changed and that they need to be aware of the risks of continuing with this method of contact. They should be advised that such contact is contradictory to this Policy and as such they are potentially placing themselves at risk of formal action being taken under the school's Disciplinary Procedure*.)

4.2 Schools should not access social networking sites in order to 'vet' prospective employees. Such practice could potentially create an un-level playing field and lead to claims of discrimination if for example the selection panel were to discover a candidate held a protective characteristic as defined by the Equality Act.

5. SAFEGUARDING ISSUES

Communicating with both current and former pupils via social networking sites or via other non-school related mechanisms such as personal e-mails and text messaging can lead to employees being vulnerable to serious allegations concerning the safeguarding of children and young people.

The Department for Education document 'Guidance for Safer Working Practices for those Working with Children and Young people in Education Settings (May 2019) states:-

12. Communication with Pupils *(including the Use of Technology)*	

In order to make best use of the many educational and social benefits of new and emerging technologies, pupils need opportunities to use and explore the digital world. E-safety risks are posed more by behaviours and values than the technology itself. Staff should ensure that they establish safe and responsible online behaviours, working to local and national guidelines and acceptable use policies which detail how new and emerging technologies may be used. Communication with children both in the 'real' world and through web based and telecommunication interactions should take place within explicit professional boundaries. This includes the use of computers, tablets, phones, texts, e-mails, instant messages, social media such as Facebook and Twitter, chat-rooms, forums, blogs, websites, gaming sites, digital cameras, videos, web-cams and other hand held devices. (Given the ever changing world of technology it should be noted that this list gives examples only and is not exhaustive.) Staff should not request or respond to any personal information from children other than which may be necessary in their professional role. They should ensure that their communications are open and transparent and avoid any communication which could be interpreted as 'grooming behaviour' Staff should not give their personal contact details to children for example, e-mail address, home or mobile telephone numbers, details of web based identities. If children locate these by any other means and attempt to contact or correspond with the staff member, the adult should not respond and must report the matter to their manager. The child should be firmly and politely informed that this is not acceptable. Staff should, in any communication with children, also follow the guidance in section 7 'Standards of Behaviour'.	*This means that adults should:* • *not seek to communicate/make contact or respond to contact with pupils outside of the purposes of their work* • not give out their personal details • *use only equipment and Internet services provided by the school or setting* • *follow their school / setting's Acceptable Use policy* • *ensure that their use of technologies could not bring their employer into disrepute* *not discuss or share data relating to children/ parents / carers in staff social media groups* *This means that education settings should:* • *wherever possible, provide school devices such as cameras and mobile phones rather than expecting staff to use their own (e.g. on school trips)*

Staff should adhere to their establishment's policies, including those with regard to communication with parents and carers and the information they share when using the internet.	

6. RECOMMENDATIONS

(i) That this policy document is shared with all staff who come into contact with children and young people, that it is retained in Staff Handbooks and that it is specifically referred to when inducting new members of staff into your school/service.

(ii) That appropriate links are made to this document with your school/services Acceptable Use Policy (see below)

(iii) That employees are encouraged to consider any guidance issued by their professional association/trade union concerning the use of social networking sites

(iv) That employees are informed that disciplinary action may be taken in relation to those members of staff who conduct themselves in a way which is contrary to the advice and guidance outlined in this Policy. If such conduct is deemed to amount to gross misconduct this may lead to dismissal.

Slyne-with-Hest St Luke's CEPS

Acceptable Use Policy / Agreement

Staff/Volunteers

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

For my professional and personal safety:

• I understand that the school will monitor my use of the school digital technology and communications systems.

• I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email, Microsoft Teams etc.) out of school, and to the transfer of personal data out of school.

• I understand that the school digital technology 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 (see Online Safety Policy)

• 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 understand that I should not write down or store a password where it is possible that someone may steal it.

• I will "lock" my laptop/desktop PC when I am away from my workstation, to avoid compromising the security of the school network.

• I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of.

• I will not connect personal devices (e.g. mobile phone) to the school's internet connection. If I do, the school's Technical Security Policy will apply and my online activity will be monitored.

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

• I will not access, copy, remove or otherwise alter any other user's files, without their express permission.

• I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.

• 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. Where these images are published (eg on the school website / Twitter) it will not be possible to identify by full name, or other personal information, those who are featured.

• I will only use social networking sites in school in accordance with the school's policies – School Twitter page only. Social media may be accessed during social time (e.g. during lunch) on personal devices that are not connected to the school network.

• I will only communicate with pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner.

• I will not engage in any on-line activity that may compromise my professional responsibilities.

• I will adhere to the schools AUP for working at home to deliver home learning

• I will inform children that any online learning will be recorded and available on the chat function for everyone to access and view, for a period of 21 days.

The school and the local authority have the responsibility to provide safe and secure access to technologies:

• When I use personal mobile devices (laptops / tablets / mobile phones etc) in 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. (See Online Safety Policy).

• I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)

• 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 try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.

• I will not install or attempt to install programmes of any type on a machine, Ora store programmes on a computer, nor will I try to alter computer settings, unless agreed by the Headteacher.

• 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 Data Policy. Where digital personal data is transferred outside the secure local 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 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 the school:

• I understand that this Acceptable Use Policy applies not only to my work and use of school digital technology equipment in school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school.

• I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include 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 digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff/ Volunteer Name:_____

Signed: _____

Date: _____