ICT Safeguarding (Including Social Media Usage for Staff) Policy

Committee Responsible for Policy: Full Governing Body

Policy written by: Miss Rachel Vidler / Miss Selina Pacey

Policy shared with staff: January 2018

Policy confirmed by the Governing Body of Linchfield Community Primary School on:

Date: March 2018
Signature: Full Governing Body
Policy to be reviewed : Every Year

INTRODUCTION

This policy sets out the following guidance for the use of ICT within Linchfield Community Primary School.

Digital Photographs:

- Staff must only use the School's own digital cameras or electronic devices to take any photographs.
- Staff should not ordinarily use any other digital device to take photographs in our School. However, if a personal camera is used, all photographs must be downloaded onto a school computer as soon as possible and deleted from the storage device/camera.
- Photographs must not be stored on any computers other than those provided by the School.
- Images should only be taken and used in line with our School policy and the wishes of parents/carers and must not be distributed outside the School network without authority.

Computer and internet use in our School:

The computer system is owned by Linchfield Community Primary School and has appropriate software to ensure safe internet use. The School reserves the right to examine or delete any files that may be held on its system or to monitor any internet sites visited.

- Activity that is found to be unsuitable or that attacks or corrupts other systems is forbidden.
- School laptops remain the property of the School at all times and as such should not be used for personal use nor should they be personalised with stickers etc.
- Users are responsible for all e-mails sent and for contacts made that may result in e-mails being received.
- Use for gambling is forbidden.
- Copyright of materials must be respected.
- Use of the computer system to access, download or upload inappropriate materials such as pornographic, racist or offensive material is forbidden.
- All computers should be locked if left unattended.
- All computers should be logged off/shut down at the end of the day.
- All laptops should be stored out of sight when the School is closed.
- ICT system security must be adhered to and no password provided by the School or other related authority must be disclosed.
- Only the approved, secure email system should be used for School business.
- Personal details such as mobile numbers and email addresses must not be given to pupils.
- Personal data i.e. information about individuals, must be kept secure and used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Headteacher or Governing Body. Personal or sensitive details taken off site must be encrypted.
- No hardware or software should be installed without reference to the ICT Manager.

Computer and internet use by the Governing Body:

- Governors will use school iPad to access governor meeting via the Trust Governor Secure Site.
- At the end of a governor meeting it will be the responsibility of all governors to shut down all information from their iPads.
- At the end of a meeting it will be the responsibility of two members of the governing body, nominated at the beginning of the meeting, to check all information is taken off the iPads and that they are shut down correctly.

Rules for Responsible Internet Use

- All Internet activity should be deemed appropriate.
- Other user's files will not be accessed without their permission.
- The School's email/internet/intranet/learning platform and any related technologies must only be used for professional purposes or for uses deemed 'reasonable' by the Headteacher or Governing Body.
- Computer discs/pen drives will not be used without prior permission.
- Internet access will only be used for agreed reasons.
- E-mail correspondence and messages sent will be polite and responsible.
- Social networking sites should not be accessed via work computers or during work hours.
- Computer files may be checked and the internet sites visited may be monitored and logged.
- All staff must adhere to the above. Any breach of these could result in disciplinary procedures and may result in the termination of their contract.

Pupils

- The School will work with parents/carers to ensure they are aware of internet use.
- Children will use only age appropriate software in the School
- All internet activity should be deemed appropriate.
- E-mail correspondence will be directed only to people who have been approved and messages sent will be polite and responsible.
- Personal details will not be shared over the internet.
- Arrangements to meet others will not be made via the internet unless a parent or carer has given permission.
- Any inappropriate materials sent to the computer must be reported to the manager.
- The internet sites visited will be monitored.
- Internet safety will be taught regularly as part of the PHSE teaching across the school.

Mobile phones

- Staff can use their personal mobile phone whilst working in school or in lessons to access school approved sites such as Scholarpack and Seesaw.
- All school information on personal devices should be shut down at the end of each session and before the member of staff leaves the school premises.
- Mobile phones should not be used for personal use in school or in lessons.
- School's telephone number should be given out to be used as an emergency contact for staff.

- Staff may use their mobile phones for personal use during breaks, which are taken in the staff room or an appropriate area separate from all pupil contact.
- Any pupils who need to bring a mobile phone to school will store these with teachers for the whole day, including time at Breakfast Club and/or Kids Club.
- Pupils will not use their mobile phones, for any purpose, whilst at Breakfast Club and/or Kids Club. They must be stored by a member of staff.
- Pupils will not take any photos on our School premises either before they give their phones to the teacher at the start of the day or as they leave the School/ playground at the end of the day. Neither will they make any contact with any other pupil on their phone either before or at the end of the day whilst on school premises.
- Pupils are not permitted to bring tablet computers or internet enabled games consoles to school at any time. This includes to Breakfast Club and Kids Club.
- Pupils will not be permitted to take mobile phones on day or residential visits.

Social Networking Sites

- Staff should at no time post anything regarding children, their parents/families or other staff at our School.
- Staff must be conscious at all times of the need to keep personal and professional lives separate and maintain professionalism whilst using social networking sites.
- Staff should not accept friend requests from a person believed to be a parent, a pupil or a recent ex-pupil except in circumstances where a member of staff has personal contact with a parent outside of school (e.g. through a club).
- No photographs from the School may be used, or ones which identify the School or children from the School
- No photographs of other members of staff to be used without their consent.
- Anyone posting remarks which breach confidentiality or are deemed to be of a detrimental nature to the School or other employees may be subject to disciplinary proceedings.
- Any employee, who becomes aware of social networking activity that would be deemed distasteful or not appropriate, should make their Leader/a member of the Senior Leadership Team aware.
- Social Networking Sites should not be used to carry out School business. Colleagues should not be contacted through such sites with relation to any school matter; school email address and/or telephone number should be used.
- All staff, visitors and volunteers to school will sign the Social Media Usage Agreement (Appendix 1)

Appendix 1.

Linchfield Community Primary School

Social Media Usage

Professional Vulnerability

A teacher can be vulnerable to unintended misuses of electronic communication. Email, texting and social media encourage casual dialogue and very often, very innocent actions can easily be misconstrued or manipulated.

Electronic messages are not anonymous and can be tracked, living forever on the internet. Social media sites archive content posted, even when deleted from online profiles. Once information is placed online, the author relinquishes control of it.

A teacher should never share information with students/parents/staff, that they would not willingly or appropriately share in a school or school-related setting.

Minimising the risk when using electronic communication and social networking?

All staff, governors, students, visitors and volunteers must adhere to the statements below:

Conduct

- Always maintain a formal and courteous and professional tone in communication with pupil and parents, ensuring professional boundaries are maintained
- Operate online in a way which would not call into question your position as a professional
- Assume that all information you post can be accessed and altered online
- Do not discuss pupils, colleagues, parents or carers online or criticise your employer or others within the school community
- Do not mention the school on social media profiles or posts
- Do not identify yourself as being associated with the school-with the exception of the professional networking site Linkedin
- Do not post online any photos of school events or photos taken within the school premises
- Do not use social media on school devices, iPads and laptops, and no social media posts should be posted on personal devices within the working day
- Never use location-based dating apps when on school premises

Communication

- Only use official channels of communication with parents/carers, eg work email addresses. When using Seesaw, do not use this as a platform for sending children or parents/carers private messages

- Do not exchange private text, phone numbers, personal email addresses or photos of a personal nature with pupils or parents/carers
- Consider that conversations held online may not be private and can be shared, therefore be aware of who may have access to what you post
- Do not communicate via email with pupils

Friend Requests

- Firmly decline student-initiated 'friend' requests from pupils, or ex-pupils under the age of 18 and do not instigate any yourself
- Notify a member of SLT if a pupil requests to follow you online and notify parents
- Use your own discretion when dealing with friend requests from parents. It is acceptable to decline these invitations. When connections with parents are made, ensure you remind parents of more formal channels which they can discuss their child's education and do not discuss any school related content via social media platforms

Security Settings

- Use the most restrictive privacy settings on social media accounts. Twitter and Instagram should be set as locked account. Facebook settings should be as private as possible
- Manage your privacy settings and keep them under review - this is particularly important with regards to photos. Remember that no privacy mechanism is 100% guaranteed.
- Use strong passwords and change them regularly
- Protect your phone/tablet/laptop with a pin, especially when in school, to protect access to its content and potential misuse
- Do not link your known work email account or mobile phone numbers to social media accounts (this allows Facebook to harvest your data and make recommendations of potential friends)

Case law is quite clear: posts on social media should not be treated as private and anything you say that brings the school into disrepute can be used by your employer as a reason to fairly dismiss you.

Linchfield Community Primary School

Social Media Usage Agreement

I, the undersigned, have read and understand the Linchfield Community Primary School Social Media Usage Policy	
I agree to adhere to the statements laid out within the policy	

Name (printed)	Signature

Date: