POLICY – Keeping staff safe online

_____

Keeping staff safe online

Staff and volunteers will continue to work in line with our school's IT policy and procedures on online safety, our staff code of conduct and acceptable use policy.

Staff working remotely should not record any personal information about families or confidential information via personal devices. Where telephone calls are being made by staff working remotely, these should be made using a work phone where possible. If a personal phone is being used to make contact with families/complete welfare checks, staff should block their phone number by dialling 141 prior to making the call.

If e mails containing personal information/confidential information are being sent remotely, staff should be reminded to password protect these before sending (sending the password via text) or encrypt the e mail before sending.

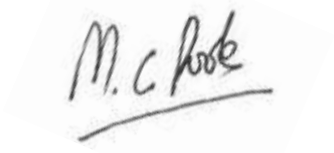
Where live lessons or video meetings are being recorded, all parties should be made aware and this should be in line with the school's data protection guidance. The data protection officer should be made aware.

Further guidance for staff working remotely can be found in the **Safer Working Practice addendum (published in April 20). SEE BELOW**

Schools should ensure any use of online learning tools and systems is in line with privacy and data protection/GDPR requirements.

Approved by Governors on 08.03.2023

Signed: Chair of Governors



Headteacher

Review date: March 2025

Relevant sections from Safer Working Practice

12. Communication with children (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. Online 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'.** 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

7. Standards of behaviour

All staff have a responsibility to maintain public confidence in their ability to safeguard the welfare and best interests of children. They should adopt high standards of personal conduct in order to maintain confidence and respect of the general public and those with whom they work. There may be times where an individual's actions in their personal life come under scrutiny from the community, the media or public authorities, including with regard to their own children, or children or adults in the community. Staff should be aware that their behaviour, either in or out of the workplace, could compromise their position within the work setting in relation to the protection of children, loss of trust and confidence, or bringing the employer into disrepute. Such behaviour may also result in prohibition from teaching by the Teaching Regulation Agency (TRA) a bar from engaging in regulated activity, or action by another relevant regulatory body. The Childcare (Disqualification) Regulations 2018 set out grounds for disqualification under the Childcare Act 2006 where the person meets certain criteria set out in the Regulations. For example, an individual will be disqualified where they have committed a relevant offence against a child; been subject to a specified order relating to the care of a child; committed certain serious sexual or physical

offences against an adult; been included on the DBS children's barred list; been made subject to a disqualification order by the court; previously been refused registration as a childcare provider or provider or manager of a children's home or had such registration cancelled. A disqualified person is prohibited from providing relevant early or later years childcare as defined in the Childcare Act 2006 or being directly concerned in the management of such childcare. Schools and private childcare settings are also prohibited from employing a disqualified person in respect of relevant early or later years childcare. The Disqualification under the Childcare Act 2006 (Regulations 2018) state that schools should make clear their expectation that staff should disclose any relationship or association (in the real world or online) that may impact on the school's ability to safeguard pupils. This applies to all staff in all schools, not just those in early or later years childcare.