CHAWTON C.E. PRIMARY SCHOOL
'Love, Courage and Fellowship'

Policy:	**Social Media policy**
Policy Date:	SUMMER 2023
Review Cycle:	3 years
Reviewer:	FGB
Approved:	SUMMER 2023
Next Review:	SUMMER 2026

Jesus said "I have come so that you might have life –
life in all its fullness." John 10:10

Jesus encouraged all his children to live life in all its' fullness. Through our core values of **love, courage** and **fellowship**, and with an enquiry approach to our inter-disciplinary curriculum, our children enjoy learning about themselves, about others and the world which we are guardians of. We nurture a love of learning, celebrate courage to persevere in learning and fellowship through collaboration and recognising each other's strengths and special qualities.

'Be kind, never give up and work together.'

1. Overview:

1.1 Chawton CE primary school recognises the benefits and opportunities which new technologies offer to teaching and learning, marketing and communication. We encourage the use of technology in order to enhance skills and promote achievement. However, the accessible and global nature of the internet and variety of technologies available mean that we are also aware of potential risks and challenges associated with such use.

1.2 This policy outlines the responsibilities of stakeholders when accessing social media, for either personal or school purposes. It supports the Staff acceptable use of IT, the Child Protection and Safeguarding Policy and Procedures, the Guidance on working with pupils, and the school's response to the Prevent Duty. It aims to ensure that organisational risks are effectively managed, in order to:

- Safeguard young people
- Protect the reputation of the school
- Protect staff and governors from exposure to legal risk.

2. Scope and Definitions:

2.1. Social media is the term used to describe the online tools, websites and interactive media that enable users to share information, opinions, knowledge and interests. Social media involves building online communities or networks, which encourage participation and dialogue. Social networking applications include, but are not limited to blogs, online discussion forums, collaborative spaces, and media sharing services. Examples include Twitter, Facebook, Instagram, Snapchat and You Tube.

2.2 The school acknowledges the value that social media can add to the school if used in a responsible and professional way. Chawton CE primary school is committed to maintaining confidentiality and professionalism at all times, whilst also upholding its reputation by ensuring employees exhibit appropriate conduct.

2.3 This policy applies to all school staff (including agency, contract workers and volunteers) and students and will come into force where there is a safeguarding, welfare, legal or reputational impact upon pupils, staff and / or the school organisation.

3. Legislation:

3.1 The school will adhere to its obligations under the legislation relevant to the use and monitoring of electronic communications, which are predominantly the Regulation of Investigatory Powers Act 2000; the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000; the Communications Act 2003; Data Protection Act 1998; the Human Rights Act 1998; the Defamation Act 1996, the Equality Act 2010 and the Prevent Duty as part of the Counter-Terrorism and Security Act 2015.

4. Data protection and monitoring

4.1 Computers are the property of the school and are primarily designed to assist in the performance of work and study duties. Therefore, staff and pupils should have no expectation of privacy when it comes to the sites they access from school computers and devices or from their personal devices via the school wired or wireless network. The school employs the use of web filters to monitor this.

4.2 The school may exercise its rights to intercept internet access under the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 for the following business reasons:

- To establish the existence of facts relevant to the school's business.
- To ascertain compliance with regulatory practices or procedures relevant to the school.
- To ensure that employees using the system are achieving the standards required.
- To prevent or detect crime.
- To investigate or detect the unauthorised use or abuse of the telecommunications systems, including using social media websites.
- To ensure effective operation of systems, e.g. to detect computer viruses and to maintain an adequate level of security.

4.3 To be able to exercise its rights, the school must make all reasonable efforts to inform every person who may use the internet systems that monitoring may take place. Staff are made aware of this through the Staff Acceptable Use of IT Policy. All pupils are made aware through initial induction, Pupil Acceptable Use of IT Policy and subsequent Computing sessions.

5. Privacy Settings and Personal Information

5.1 Default privacy settings for some social media websites allow some information to be shared beyond an individual's contacts. In such situations, the user of the site is personally responsible for adjusting the privacy settings for the account. Information available on social media sites could be produced as evidence by either a school or employee, should it be necessary either as part of school procedures, or in legal proceedings.

5.2 Therefore, it is vital that employees and pupils are strongly encouraged to review their access and privacy settings for any social media sites to control, restrict and guard against who can access

the information on those sites. Even if privacy and security settings are utilised, anything posted on social media sites may be made public by onward transmission.

5.3 Social media offers the ability to share personal information rapidly and easily. Employees should be aware of the importance of setting and protecting secure passwords and personal information to reduce the risks of abuses such as identity theft.

5.4 To avoid identity theft, employees are advised to refrain from publishing any personal or sensitive information on social media websites, e.g. date of birth, home address, telephone number or any information related to personal bank accounts.

6. Acceptable use of social media

6.1 The school's IT Systems are first and foremost business tools, and as such personal usage of the systems is a privilege and not a right. The school reserves the right to make reasonable and appropriate use of social media websites where this is part of the normal duties of their work. It is an important part of how the school communicates and interacts with its community.

6.2 The school accepts that staff may wish to use social media channels as a way of communicating both internally and with external agencies. It is recognised that there are clear educational and marketing opportunities provides by these technologies. However, use of social media should be restricted to the terms of this policy:

a) Staff will conduct themselves in accordance with other school policies and procedures;
b) Be professional, courteous and respectful as would be expected in any other situation. Think carefully about how and what activities are carried out on social media websites;
c) It is recognised that social media is used for official school purposes and may be used within curriculum areas for pedagogical reasons. Staff use of social media for school purposes must be transparent and accountable. Staff must not form personal relationships with any pupils, or ex-pupils under the age of 18 and must ensure that professional boundaries are maintained at all times. Entering into such relationships through social media websites may lead to abuse of an employee's position of trust, and breach the standards of professional behaviour and conduct expected at the school. It is therefore school policy that more than one teacher have access to a school social media account, and that the line management is informed of any account details;
d) Staff will remember their statutory welfare, safeguarding and prevent duty when using social media and report any inappropriate behaviour, action or comment using the school's safeguarding and welfare procedures.

7. Unacceptable use of social media

7.1 It is recognised that social media is increasingly important within education, both within a pedagogical and marketing context. However, either in a professional or personal capacity, within or outside the workplace, staff and pupils must not conduct themselves inappropriately. The following are examples of inappropriate conduct (this is intended for illustrative purposes and is not exhaustive)

a) Engaging in unlawful activities or attempting to persuade others to engage in unlawful activities;
b) Engaging in activities that contravene other school policies and procedures. This can includes activities considered bullying, harassment or discrimination;
c) Engaging in activities that have the potential to bring the school into disrepute or that may have the potential to cause serious harm to the business;
d) Breach of confidentiality by disclosing any personal information;

e) Posting or uploading inappropriate comments, images, photographs and/or video clips about colleagues or ex-colleagues, pupils or ex-pupils, parents or other external agencies;
f) Publishing defamatory and/or knowingly false material about the school, other employee or students;
g) Use of offensive, derogatory or intimidating language which may damage working relationships;
h) Pursuing personal relationships with any pupils, or ex-pupils under the age of 18;
i) Participating in any activity which may compromise the individual's position at the school;
j) Knowingly accessing, viewing or downloading material which could cause offence to other people or may be illegal;
k) Posting any material that breaches copyright legislation;
l) Knowingly contact, promote or access extremist and / or terrorist groups and / or materials.

8. Roles and Responsibilities:

8.1 The Designated Safeguarding Lead (DSL):

The DSL is responsible for ensuring staff development and training is provided on safeguarding including Prevent, recording incidents, reporting any developments and incidents to the relevant bodies and liaising with the local authority and external agencies to promote and ensure safety within the school community. For more information, please refer to the school's Child Protection and Safeguarding Policies and Procedures.

8.2 School Staff:

- All staff are responsible for using the school IT systems and mobile devices in accordance with the school Staff acceptable use of IT and the Social Media Policy, which they must actively promote through embedded good practice. Staff are responsible for displaying a model example to students at all times.

All digital communications must be carried out in a professional manner and contain appropriate content at all times. Staff must use the school's official email account for communication with parents and for school related business. Staff must not give their personal phone number to pupils or parents to correspond via text message with them.

All staff should apply the relevant school policies and understand the incident reporting procedures. They should understand their role in safeguarding and the prevent duty. Any incident or concern that is reported to or discovered by a staff member must be reported to the Designated Safeguarding Lead or Deputy Designated Safeguarding Lead.

8.3 Pupils:

Pupils are responsible for using the school IT systems and mobile devices in accordance with the Home-school agreement which they must agree to, and the e-Safety Policy. Pupils are expected to seek help and follow procedures where they are worried or concerned, or where they believe an e-Safety incident has taken place involving them or another member of the school community. Pupils must act safely and responsibly at all times when using the internet and/or mobile technologies.

8.4 Parents:
Parents are responsible for discussing age appropriate computer/internet allowance with their children and monitoring children's computer/internet activity at home.

9. Prevention and Security

9.1 The school will do all that it can to make sure the school network is safe and secure.

9.2 Staff will be asked to review the Social Media Policy as part of induction to the school. Further safeguarding including prevent training will be delivered to all or staff or groups of staff as appropriate. The Staff Acceptable Use of IT Policy is displayed and must be agreed to as part of staff induction.

9.3 The Staff acceptable use of IT is reviewed and agreed to by pupils upon enrolment for pupils. Pupils will receive guidance on the safe use of IT systems and equipment, including e-Safety, through e-safety lessons. Issues associated with social media apply across the curriculum and pupils should receive guidance on what precautions and safeguards are appropriate, when making use of the internet and technologies. Pupils should also know what to do and who to talk to where they have concerns about inappropriate content. Within classes, pupils will be encouraged to question the validity and reliability of materials researched, viewed or downloaded. They will also be encouraged to respect the copyright of other parties and to cite references properly.

9.3 Every effort will be made to keep security software up to date. Appropriate security measures will include the use of enhanced filtering and protection of firewalls, servers, routers, work stations etc. to prevent accidental or malicious access of college systems and information. Digital communications, including email and internet postings, over the school network, can be viewed in line with the school's Social Media Policy and statutory duties.

10. Incidents and Reports

10.1 Any breach of this policy, including inappropriate conduct of the kind listed in section 7 above, or of a similar nature, and any excessive personal use of social media websites will be dealt with in accordance with the school disciplinary or safeguarding procedures (as relevant).

<u>Guidance for staff on: Use of Specific Social Media Technologies</u>

Introduction

Chawton CE Primary School recognises the benefits and opportunities that new technologies offer to teaching and learning. We encourage the use of technology in order to enhance skills and promote achievement, and staff should feel that they can use electronic media such as social networking sites to communicate with others. It is essential, however, that you take care with the information you make public and remember that once a comment or posting is made, it may not be possible to take it back; there will always be a permanent digital record of it.

As a school employee, you should remember your public role and always consider how your conduct could affect your professional reputation and the reputation of Chawton CE Primary School.

This guidance is intended to give you a number of simple hints to assist you to keep your information safe when using electronic media and to protect you from putting yourself and your employment at risk.

What is a Social Network Service?

Social networking encourages communication and the sharing of information. Social networking websites are used regularly by millions of people and focus on building online communities of

people who share interests and/or activities or who are interested in exploring the interests and activities of others.

Currently the most popular social networking sites are Facebook, LinkedIn, Instagram, Snapchat and Twitter:

Using Facebook and Linkedin
In order to stay safe, you should:

- Remember your role as a member of school staff and that you should always consider how your conduct could affect your professional reputation and the reputation of the school;
- Discuss new ideas for any new accounts and obtain permission from the Headteacher before initiating an account that represents the school;
- Create separate 'professional' and 'personal' profiles and use them accordingly. Keep your professional and personal life separate – you should not become 'friends' with any of your current or former pupils on your personal social networking site;
- Ensure login details for professional accounts are shared with your line manager. Staff must discuss and obtain permission from the Headteacher before initiating an account representing the school;
- Set your personal social networking profile to private so that only your chosen friends can see any photos you publish on it;
- Think before you post any photos of yourself (or comments) on the Internet - ask yourself if you would be comfortable with others such as your colleagues, manager, pupils, their parents etc. seeing them;
- Make sure that you use a strong password with a combination of numbers and letters and that you keep this password safe. If you use a public or shared computer to access you social networking site (outside of school), cancel any auto-login or 'remember me' functions and always make sure you log out at the end of the session. This will prevent anyone from accessing your account;
- Where pictures / videos are posted from professional accounts, make sure you have permission from other people in the picture / video. Please note that all parents confirm their permission to be used in marketing materials when signing up at enrolment except where they have chosen to opt out.

Using Instagram

Instagram is a free online social networking site that allows you to share daily life and important events through pictures. Pictures can be digitally altered with filters that the Instagram team provides.

Using Snapchat

Snapchat is a social media app that allows people to send and receive images and videos that disappear within a certain time frame upon being viewed. This is designed to create spontaneity and minimise a digital footprint. However it has been shown that certain apps can remove this function and it can even be gotten around in a low tech fashion by people taking pictures of their phone.

Using Twitter

Twitter is a free social networking and micro-blogging service that enables users to send and read messages known as *tweets*. Tweets are text-based posts of up to 280 characters displayed on the author's profile page and delivered to the author's subscribers who are known as *followers*. Senders can restrict delivery to those in their circle of friends or, by default, allow open access. Users can

send and receive tweets via the Twitter website, Short Message Service (SMS) or external applications.

In order to stay safe when using Twitter for professional reasons, you should:

- Check who is following you. This will enable you to block anyone you do not wish to see your "tweets" (updates). Once you've logged in, Twitter shows your home page. Click on "followers" in the upper right-hand menu. There you'll see a list of everyone who has subscribed to be updated whenever you post something. You have three options for each follower: You can click their picture to see their own Twitter page; you can choose to follow them as well; or you can block them from seeing your updates or "tweets". You may want to block colleagues and pupils, etc from seeing your updates if you are posting personal items.
- Set your privacy settings: Again, this will limit who sees your updates and also enable you to change your user name so it is not your actual name. In the top right sidebar menu on Twitter there is an item called "settings." Go here to control what others can find out about you. You can also protect your tweets so only your followers can see what you post.

Using Bluetooth technology

Blue tooth technology eliminates the need for wires that tangle our everyday lives. Streaming music and connecting devices are just a few of the powerful capabilities of Blue tooth technology. Bluetooth exists in many products, the Wii, PlayStation 3, modems, headsets and mobile phones. The technology is useful when transferring information between two or more devices that are near each other in low-bandwidth situations. Bluetooth is commonly used to transfer sound data with telephones (i.e., with a Bluetooth headset) or byte data with hand-held computers (transferring files).

In order to stay safe with Bluetooth, you should:

- Check whether or not your device has a bluetooth facility;
- Make yourself familiar with how to switch the bluetooth facility on and off. If you have a mobile phone with bluetooth technology, you could be at risk of 'bluejacking' (where another Bluetooth user in your vicinity can send you a message without knowing your number) or 'bluesnarfing' (where another Bluetooth user can access your mobile and steal things like your contact list, emails, texts and photos).
- It is recommended that you switch off your bluetooth to prevent unwanted or accidental communication with pupils.

How do I get offensive content taken down?

If upsetting or inappropriate images or information is found on the Internet the first person to contact is the person who is responsible for posting the material. If this is not possible then you can contact the service providers and request the information to be removed.

The following contact details will help you in the event that you discover any comments or postings which you consider to be offensive:

- FACEBOOK – Reports can be made by clicking on the 'Report' link located on pages throughout the site, or by email to abuse@facebook.com or www.facebook.com/safety
- TWITTER – To report violations of privacy or threatening behaviour guidelines are published on http://help.twitter.com/forums/26257/entries
- YouTube – Logged in YouTube members can report inappropriate content by using the 'flag content as inappropriate' function which appear under every video.