

Social Media Policy



Updated October 2019

Contents

Introduction	4
What is social media?	4
Social media and the law	4
Sunnyside Primary School’s social media presence.....	5
Safeguarding children and families.....	5
An introduction to popular social media platforms.....	6
Twitter.....	6
Youtube.....	6
Snapchat:	6
Instagram	6
Parent/Carer Responsibilities:	7
Personal use.....	7
Social media risks	7
Monitoring	7
Common platforms, age restrictions and potential risks	7
Reporting	8
Parent Council:.....	9
Pupil Responsibilities	10
Monitoring:	10
Reporting:	10
School staff responsibilities	11
Safeguarding	11
Posting media through authorised channels	11
Teaching Digital Citizenship	12
Monitoring	12
Reporting	12
Data Protection compliance	12
Senior Leadership Team responsibilities	13
Safeguarding	13
Posting media through authorised channels	13
Monitoring	13
Reporting and Investigating.....	13
Social Media and Professional Vulnerability.....	14
Legal implications.....	14

Fitness to teach/work implications.....	14
Minimising risk.....	14
Social Media Content and Acceptable Use Overview.....	16
Online Safety Charter.....	17

Introduction

Social media offers new channels for engagement and collaboration within, and more importantly beyond, our own school. Many teachers and professionals use social media to engage in learning and reporting, often without any difficulty. However, registered teachers and others should be aware of challenges and potential ramifications associated with the use of social media.

It is of utmost importance that parents and carers are aware of their responsibilities when considering the use of social media outwith the school, and understand the risks that social media can present to our pupils. Parents should be aware of the school's use of social media and acceptable online conduct when communicating with Sunnyside Primary School and its staff.

Pupils have a duty to follow our online safety charter whilst attending Sunnyside, and a responsibility to keep themselves safe with the assistance of trusted adults. Pupils should also recognise the importance of responsible online conduct when communicating with peers.

This document seeks to clarify the potential dangers of social media use, provide guidance on acceptable use and reporting structures for any incidents that may occur.

This policy has been developed to align with UK and Scottish law, Clackmannanshire Council guidelines and GTCS guidance.

What is social media?

Social media are "...websites and computer programs that allow people to communicate and share information on the internet using a computer or mobile phone"

(Cambridge Uni. Press, 2019)

Social media and the law

Criminal offences define acts (or omissions) which are so harmful that the wrong is thought to be against the state rather than the individual who has suffered the act; the state prosecutes and, on conviction by a court, the state punishes, by deprivation of liberty, fine or other means.

When harmful acts are committed using social media, the social media is simply a platform for human beings to behave or misbehave; it is not about the medium, it is about the offence.

Harassment, malicious communications, stalking, threatening violence, incitement are all crimes and have been for a long time.

Current law that can be applied to the use/misuse of social media:

- The Equality Act 2010
- Protection from Harassment Act 1997
- Contempt of Court Act 1981 – relating to a breach in anonymity.
- Sexual Offences Amendment Act 1992
- Malicious Communications Act 1988
- Communications Act 2003

At the time of publication it is worth noting that the UK government is currently proposing legislation that seeks to make social media companies more accountable for content published on their platforms. This does not however, diminish individual responsibility for actions that may result in prosecution as described above.

Sunnyside Primary School's social media presence

Sunnyside Primary School has a very active online presence with our website forming the core of this. This is supplemented through additional social media channels such as Twitter, YouTube and WordPress Blogs (the school website).

Pupil Learning Journals are not, for these purposes, classed as social media as they are a direct reporting facility between parent, pupil and teacher. Further guidance on this can be found in the Learning Journals Policy, 2018.

Whilst the Senior Leadership Team monitor content on the official school channels it is important to recognise that information is often shared by third parties including the Parent Council Facebook and Community Council. The school does not manage content shared on these channels.

Safeguarding children and families

Each year, Sunnyside Primary School will ask all staff and families to complete a confidential data check, allowing us to update our records. Part of this check is to obtain your position on the use of photos and videos, of your child(ren), for school purposes.

We are committed to the safety and wellbeing of the young people, and their families, in our care and our responsibilities surrounding confidentiality and the use of data.

An introduction to popular social media platforms.

Twitter

Twitter is one of the largest social networking sites with over 300 million active accounts. Twitter relies on short burst of information, with a strict character limit of 280 characters, although tweets can be strung together for more information.

Twitter will allow the use of text, photos, inserted videos and hyperlinks (websites) and are viewable by “followers” and are searchable unless you have a protected account.

The Sunnyside Primary School account (@sunnyside_ps) has over 800 followers, including parents, fellow schools, educational bodies and former pupils. It is one of our most active and well utilised reporting tools.

Tweets can be deleted however they are also archived, it is important to remember that once information is put online it may no longer be private. We do not encourage the use of direct messaging unless there is no other way of contacting the school. Direct messages are seen by the recipient only and are not public.

For further information on Twitter please see: <https://help.twitter.com/en/twitter-guide>

Youtube

Youtube is immensely popular with over 23 million channels and over 1.8 billion users. Its primary purpose is to host videos that have largely been created by individuals rather than TV stations or film producers, however its commercial popularity is increasing as many users are paid to share advertisements and promote products.

When using YouTube, it is important to note that the publisher will choose whether or not to restrict content, and whilst ages may be recommended these are not enforced at present. Youtube will also recommend videos to watch after your selection has played and these may not always be suitable.

Snapchat:

The Snapchat app lets you send photos, short videos or messages to your friends. Pictures and videos, known as Snaps, usually appear temporarily before disappearing, though they can be captured via screenshots. The Stories feature lets you share Snaps in a sequence for up to 24 hours. Using the Discover screen lets you watch Stories from friends, celebrities and brands.

Instagram

Instagram is a picture and video sharing app. Users can post content on their profile grid or to their stories, which last 24 hours. You can follow your friends, family, celebrities and companies on Instagram. Instagram also has a live streaming feature.

TikTok

TikTok (formerly called Musical.ly) is a social media platform that lets you create, share and discover 15 second videos. You can use music and effects to enhance your videos and you can also browse other people’s videos and interact with them.

Parent/Carer Responsibilities:

Personal use

The school respectfully asks that if you have any comments or complaints about a member of staff, another parent or pupil or about a school policy, that you come and talk to us about it. Please raise any issues or concerns with your child's teacher or a member of the SMT. Please do not post anything derogatory or discriminatory online which 'names and shames' any individuals or brings the school into disrepute.

We will contact the police if a crime is committed in the course of social media use, including targeted harassment, abuse and or bullying.

For further information and guidance please see here: <https://www.npfs.org.uk/2018/05/clicked/>

Social media risks

Recent reports from Ofcom have found that a growing number of children under the age of 11 are registering for social media accounts despite minimum age limits. Figures at the time of publication estimate that 18% of eight to eleven year olds have their own social media profiles and accounts. The same report found that less than a third of parents who knew their child had an account were unable to correctly state the age restrictions.

Monitoring

If your child or teenager uses the internet, you should take steps to keep them safe online.

There is no single way of doing this and advice can vary depending on the age of your child.

Some common advice includes:

- using parental control software
- using a secure internet connection
- encouraging your children not to give out personal information online
- encouraging your children to think about what they post
- asking your children to tell you about any inappropriate content they find

Our website provides some advice and further links on monitoring your child's internet access. The NSPCC website www.net-aware.org.uk provides clear guidance on all social media platforms.

Common platforms, age restrictions and potential risks

Name	Age requirement	Risk Profile
Youtube	13+	<ul style="list-style-type: none">• High Risk of sexual content, violence and hatred, bullying, suicide and self-harm, drink drugs and crime.• Significant magnification of risks if pupils are creating and sharing content.
Twitter	13+	<ul style="list-style-type: none">• High risk of sexual content, violence and hatred and bullying.• Medium risk of suicide and self-harm and drink, drugs and crime.• Location data can be shared on Twitter, therefore magnifying risks.

Facebook and Messenger	13+	<ul style="list-style-type: none"> • High risk of sexual content, violence and self-harm, bullying, suicide and self-harm and drink, drugs and crime. • Location data can be shared, creating significant risk.
Instagram	13+	<ul style="list-style-type: none"> • High risk of sexual content and bullying. • Medium risk of violence and hatred, suicide and self-harm and drink, drugs and crime.
WhatsApp	16+	<ul style="list-style-type: none"> • Medium risk of sexual content, violence and hatred, bullying. • Low risk of suicide and self-harm and drink, drugs and crime.
Snapchat	13+	<ul style="list-style-type: none"> • High risk of sexual content and bullying. • Medium risk of violence and hatred, suicide and self-harm and drink, drugs and crime. • Snapchat can map precise locations where posts are created/shared therefore magnifying risk.
TikTok	13+	<ul style="list-style-type: none"> • Inappropriate language and contact from strangers. • Video and photo sharing magnifies risk of inappropriate contact and content.

All of these platforms have are privacy settings that can help lower risks, however we recommend that no child below the age requirement is allowed to use these platforms with their own account, or utilise someone else’s account without strict adult (parent/carer) supervision.

Reporting

Parents must inform school of any change in circumstance that may impact on the schools ability to utilise images or media content associated with their child. Whilst the school does conduct annual data checks it cannot be held responsible if these are not returned.

Whilst the school Twitter and website are closely monitored, sometimes, you may spot something of concern, in this case we ask that you report this to school staff via one of the following methods:

- **Twitter: Direct Message (DM) the school account @sunnyside_ps**
- **Email: sunnyside@edu.clacks.gov.uk**
- **Contact us page on the website: sunnyside.clacks.sch.uk**
- **Telephone: 01259 452 319**
- **Face to face – report your concerns directly to a member of staff.**

A member of the Senior Leadership Team will investigate any concerns regarding our social media and report back to you. During this communication period a Senior Leadership Team Member may use their work email address, however we request that these are not shared or utilised for other purposes.

We ask that evidence of the concern (dated and timed screenshots/photos) are shared with the Senior Leadership Team if requested and existing reporting and blocking features are utilised on social media platforms when outwith school control.

Parent Council:

Please note that whilst our Parent Council are involved in promoting school activities and events, they are not a reporting body/channel. There is guidance available to all Parent Councils to assist in the use of social media and online communication, available from the NPFS here:

https://www.npfs.org.uk/wp-content/uploads/2018/06/npfs_social-media_booklet_E.pdf

Pupil Responsibilities

Monitoring:

In accordance with the Sunnyside Online Safety Charter (Appendix 2) all children in Sunnyside should be aware of their responsibilities as a digital citizen. Pupils who see/ access anything unusual or inappropriate online should report this to a trusted adult.

Reporting:

Pupils at Sunnyside should share any concerns with any staff or parents, who will investigate the matter following established child protection protocols.

School staff responsibilities

In line with our commitment to protecting our young people it is paramount that we evaluate and monitor our online practices in line with Clackmannanshire Council guidance and legislation.

Safeguarding

Working with young people, it is the responsibility of all staff at Sunnyside to ensure that we consider the individual needs and rights of all children within our care. Therefore we cannot provide any personal information, or images, of pupils or families without prior consent.

Annual data checks must be reviewed before any image or media featuring a child can be used, if no data check is returned we will assume that no permission has been given.

Any staff member taking, sharing or storing photos should do so using Clackmannanshire Council authorised equipment; failure to do so can risk data breaches and leave employees open to allegations of misconduct. Staff should not use their own devices as this heightens the risk of a data breach.

Some areas and events within our school community may pose a higher risk to pupils and it is imperative that staff do not share photos from these without checking with the appropriate social media permissions with the designated class teacher/ lead professional. Such events/areas include:

- Whole school events.
- Public engagements and visits.
- Nurture bases/social groups.
- Cross school committees.
- Support for Learning sessions.
- Targeted support work.
- Meetings.

Areas/activities where recording of any type is barred include:

- Changing areas or at changing times.
- Bathroom facilities.
- Swimming.

Any staff member utilising school social media must complete Clacks Academy Social Media and GDPR e-Learning modules.

Posting media through authorised channels

Class Teachers and Early Education and Childcare Workers are permitted to utilise the school Twitter account and upload information to the school website, once appropriate training has been completed. Others wishing to post via the school account must seek permission from a member of the Senior Leadership Team and complete all relevant e-Learning.

When posting to Twitter or the school website the following rules apply:

Acceptable Content	Not Acceptable
<ul style="list-style-type: none">• Class work – unnamed• School trips• Class events• School events – see additional risks above.	<ul style="list-style-type: none">• Personal opinions including any regarding the school, other colleagues or the authority.• Any visibly named work.• Photos of children without written consent from a parent or guardian.

<ul style="list-style-type: none"> • Retweets of council organised events such as ActivClacks, Library workshops. • Outgoing sharing of information. • “Overhead/over the shoulder” photos. • Images that positively reflect on the young person’s involvement in the activity. 	<ul style="list-style-type: none"> • Photos of any individual without consent. • Full face photos of pupils/groups. • Names of children. • Copyrighted content. • Photos of activities where there is a heightened risk of misuse (eg. swimming). • Direct messaging or responding to tweets without Senior Leadership Team consent.
---	--

Teaching Digital Citizenship

It is the duty of all teachers to address cyber resilience and internet safety as part of the curriculum, this should be recapped every term with pupils, and as events of concern come to light through pupil discussions, and where appropriate child welfare protocols should be followed – online risks are as important as real world experiences.

The Sunnyside Online Safety Charter is to be shared in all classes and strictly enforced.

Monitoring

When children are using devices it is the responsibility of the class teacher or supervising staff member to ensure that content is appropriate, reporting any concerns.

It is the responsibility of class teachers to ensure that images and content shared are in line with the provided guidance (within this document). If a staff member has any concerns about content shared or any communication via social media, this should be raised with a member of the Senior Leadership Team immediately.

Reporting

Any misuse or concerns regarding the use of social media by a pupil, parent/carer or colleague must be reported to the Senior Leadership Team.

Data Protection compliance

All staff must complete GDPR/Data Protection Clacks Academy e-learning modules.

In order to comply with GDPR, the Data Protection 2018 Act and protect the individual rights of all, social media permissions for children must be kept in Personal Pupil Records, and further parental permission should be sought if photos are to be shared by external agencies. Pupil records must be checked prior to photos being taken and, if consent has not been given, then the photo must not be taken. Or in the case of a group/class photo, the child(ren) excluded.

In order to share images of families, adult visitors or colleagues you must obtain their permission; this can be actioned through written or verbal agreement.

All staff are responsible for GDPR compliance and adherence to Clackmannanshire Council guidance.

Senior Leadership Team responsibilities

The Senior Leadership Team comprises of the Head Teacher, Depute Head Teacher(s), Principal Teachers and Senior Early Years Workers.

Safeguarding

The Senior Leadership team have overall responsibility for the safeguarding of pupils, staff and families at Sunnyside Primary School. School policies and protocols should be reviewed and enforced to ensure the safeguarding of all and ensure compliance with local authority and guidance and relevant legislation.

Posting media through authorised channels

The Senior Leadership Team must adhere to the same guidance provided to all staff regarding social media, however may also use the school YouTube channel to host video content such as SparkNotes and Adobe Videos.

Content uploaded to YouTube should be “unlisted” and then shared via the school website – embedding the URL into the appropriate page/post.

Monitoring

The Senior Leadership team must review content posted to school social media channels on a regular basis and report any incident or concern to the Head Teacher, taking action as required and directed by the Head Teacher.

A record of any incident, including screenshots and/or communications is to be provided to the Head Teacher.

Reporting and Investigating

Where breaches may have occurred, the Senior Leadership Team must report this to the Head Teacher who will direct and facilitate any subsequent investigation within the school or with appropriate external agencies and parties as necessary.

Social Media and Professional Vulnerability

As professionals it is important that teachers and other school staff are aware that social media can leave you vulnerable to intended misuse. **Any social media accounts (Twitter) that are used for professional dialogue (liking school posts, sharing Authority and school events etc...) should be solely used for this purpose to avoid and minimise risks of professional vulnerability. Separate personal accounts may be used, however these should not be linked to school accounts/communications.**

All electronic messages and social media are not anonymous and can be tracked and live forever in the internet. Social media sites will often archive content posted, even when deleted. Once information is online, the author must understand that they have relinquished control.

The personal use of social media is increasing amongst professionals with sites such as Facebook, Twitter and Instagram. It is important to understand that although the GTCS states that “teachers are individuals with private lives...off duty contact may have a bearing on their professional life. Therefore sound judgement and due care should be exercised as conduct which may not directly relate to pupils may be relevant to a teacher’s fitness to teach.

Legal implications

Unwise online behaviour can result in criminal action, or in some cases, civil action brought by others and therefore requires caution. The GTCS code of Professionalism and Conduct draws attention to the potential impact of criminal convictions on registered teachers, and the PVG scheme outlines how this may affect other colleagues.

Fitness to teach/work implications

The GTCS framework puts the protection of children and vulnerable persons first, as does the PVG scheme. These structures have allowed a culture of trust in school personal to develop between employees and the public. Therefore all complaints are considered fairly and in the same way, regardless of association with

Example behaviours that have warranted disciplinary measures:



- Inappropriate electronic communication with pupils, colleagues and parents/carers, including instant messaging and SMS.
- Posting of sexually explicit imagery.
- Grooming – the establishment of an inappropriate relationship with a pupil.
- Use of inappropriate YouTube content within the classroom.

Minimising risk

- Comply with the authority guidance on social media, as prescribed in the Clacks Academy e-learning course.
- Always maintain a formal and courteous and professional tone in communicating with pupils and ensure professional boundaries are maintained.
- Do not exchange personal contact details with pupils.
- Firmly decline any pupil request to befriend you via social media and encourage all parents to use formal agreed channels of communication.
- Manage and review your own privacy settings.
- Consider that online discussions and communications may not be private.
- Do not discuss pupils, families, colleagues, and your workplace online or criticise your workplace or the wider authority.

- Use strong passwords and regularly update them, this prevents potential misuse.
- Bring forward any matter of concern to a member of the senior management team. This includes online comments, photos, posts or other content that makes you feel uncomfortable.

Social Media Content and Acceptable Use Overview

 Acceptable Content	 Not Acceptable
<ul style="list-style-type: none"> • Class work - unnamed • School trips • Class events • School events - see additional risks above. • Retweets of council organised events such as ActivClacks, Library workshops • Outgoing sharing of information • "Overhead/over the shoulder" photos • Images that positively reflect the young person's involvement in the activity 	<ul style="list-style-type: none"> • Personal opinions including any comment regarding the school, other colleagues or the authority • Any visibly named work • Photos of children without written consent from a parent or guardian • Photos of any individual without consent (adults) • Full face photos of pupils/groups • Names of children • Copyrighted content • Direct messaging or responding to tweets without Senior Leadership Team consent • Photos of activities where there is a heightened risk of misuse (eg. swimming)



Sunnyside Primary Online Safety Charter



SAFE

Don't give away any personal information online without permission from a trusted adult. Including your real name, address, phone number, email, any photos or even your school.



MEET

Remember unless you can be 100% sure you know someone in real life, they are a stranger. Meeting up with them and sharing personal information can be dangerous.



WARE

Think about what you are clicking on. Don't open messages, emails or files sent by people you don't know. Turn off your webcam and mic when you're not using them.



EAL

It is important to act online as you would in real life. Be respectful of others, even when you don't agree. Trolls belong in fairytales. If someone is mean - block them and report it.



ELL

It is very important to tell a trusted adult if you see anything you don't think is right. Making mistakes can happen, but fixing them takes help—it's important to tell and stay safe.

Did you know.?

WhatsApp, Facebook, Twitter, Instagram all have an age limit. You must be 13 years or older to use them.



Using them underage can be harmful



Created by your Digital Leaders