

Giles Junior School



Achieving Excellence through Leadership

Social Media Policy (Including acceptable user agreements)

Document Details	
Approving Body	FGB
Author	Giles Junior School
Committee Responsibility	Resources
Scheduled Review	Annually
Date of Policy	September 2026
Next Review	September 2027

1.	Introduction	3
2.	What is social media?	3
3.	Types of social media	3
4.	Personal use of social media within working time	3
5.	Business use of social media	3
6.	Prohibited use of social media	4
6.1.	Inappropriate use	4
6.2.	Safeguarding and social media	5
6.3.	Use of emojis, GIF's and Memes	6
6.4.	Absence from work and use of social media	6
7.	Guidelines for responsible use of social media	5
8.	Monitoring	7
9.	Breach of this policy	7

1. Introduction

The aims of this policy are to:

- enable appropriate use of social media in a safe and secure manner
- safeguard employees in their use of social media and ensure they do not make themselves vulnerable
- minimise the risks to the school through use of social media.

This policy applies to use of social media for business purposes as well as personal use that may affect us in any way. This includes conduct outside working hours where use of social media may impact on the school, its reputation, safeguarding obligations, or the trust and confidence required in the employment relationship. It covers all employees, consultants, volunteers, and agency workers.

This policy does not form part of any employee's contract of employment, and it may be amended at any time. We may also vary this policy as appropriate in any case.

2. What is social media?

For the purposes of this policy, social media is any online platform or app that allows parties to publish information, share content and interact with others either to a wide audience or through private conversations, such as private messages.

Social media is the term used for internet-enabled tools used on computers, tablets, smartphones and other smart devices etc. to allow people to share information, ideas and views.

3. Types of social media

This policy covers all social media platforms, including, but not limited to:

X, Facebook, Instagram, LinkedIn, YouTube, TikTok and message boards.

It also includes any website where you can contribute or edit content and instant messaging services i.e., WhatsApp, Snapchat etc.

This policy also applies to any other existing or new social media platform not mentioned, whether internal or external or used on a personal or work device.

All forms of social media use are covered by this policy, this can include but is not limited to; posting comments, pictures or videos, blogging, using forums, sending private messages, endorsing other people's content, re-tweeting/circulating posts or adding/editing content on a website.

If it can be determined from your account that you work for us (either visually, verbally or written), we ask that you make it clear that any content and views are your own. Confirming this point does not make you exempt from following this policy.

Please include "these views are my own and not that of my employer" on your profile.

4. Personal use of social media within working time

You must limit your personal use of social media on your own equipment to rest breaks such as lunch or break times. The use of personal devices must be discreet and not in the presence of pupils. Personal use may not interfere with employment responsibilities or productivity and must comply with this policy.

Any permitted personal use of social media must always be appropriate, discreet, and compliant with this policy, safeguarding requirements and professional standards.

5. Business use of social media

If you are contacted for comments about us for publication anywhere, including in any social media outlet, the enquiry should be directed to the Headteacher, and you should not respond without written approval.

6. Prohibited use of social media

You must avoid making any social media communications that could damage our interests or reputation, even indirectly. This includes content posted, shared or endorsed intentionally or recklessly, whether publicly or through private messaging, where it may reasonably be expected to cause harm or reputational damage.

You should not use social media in a way that breaches any of our policies, the law, or any other regulatory requirements.

6.1. Inappropriate use

Social media use is permitted as long as it does not involve unprofessional or inappropriate content and does not interfere with us or your role or responsibilities. Inappropriate use includes, but is not limited to:

- any content that could be viewed as malicious, abusive, offensive, obscene, threatening, intimidating or contain nudity or images of a sexual nature.
- discrimination (e.g., racism, homophobia etc.)
- swearing (both verbal and gestured) any content including explicit lyrics.
- making or endorsing harmful or derogatory comments.
- any threatening behaviour that may cause harm to others or our interests or reputation.
- bullying and harassment.
- making false or misleading claims/ statements.
- impersonating colleagues or third parties.
- posting or sharing information that could jeopardise our confidentiality, particularly regarding sensitive topics related to us, such as our performance, internal disputes involving pupils, parents, or employees.
- disparaging us, its employees or any third party.
- sharing sensitive or personal information about us or employees that should not be discussed or shared or is personal data protected under data protection legislation. For example., absence information or contact details.
- endorsing, liking, sharing or engaging with content that could reasonably be considered offensive, speculative or likely to cause reputational damage to us. This includes adding or commenting on speculation.
- sharing login details or allowing others to post on your behalf.
- using your professional email address for a personal social media account.
- create social media accounts representing us without prior authorisation.
- expressing opinions on behalf of us or using our logo or other trademarks without express authorisation.

These examples include creating, endorsing, liking, posting, retweeting, sharing, direct messaging or sending any statements, photos, videos, audios, or messages. They also include speaking and/or lip syncing to other creators' content and any music used.

You should never provide professional references or endorsements on behalf of us for other individuals without the express authority of the Headteacher including on social or professional networking sites. Such references, positive and negative, can be attributed to us and create legal liability for both the author of the reference and us.

6.2. Safeguarding and social media

You must not abuse your professional position with pupils on social media. Examples of abuse of position include, but not limited to:

- Accepting any former pupil under the age of 18, or any current pupils, as friends, or requesting such friendships
- Communicating personally with pupils.
- Posting photographs of pupils on sites not owned by us.
- Commenting about or naming pupils.
- Staff must not seek out or engage with pupils via personal social media accounts, including searching for pupils or viewing their profiles unless there is a legitimate safeguarding concern and this is authorised.
- Engagement with ex-pupils – staff should exercise caution in relation to ex-pupils, particularly those who have recently left the school or who may still be under the age of 18. Engaging with ex-pupils through personal social media accounts, or forming personal relationships with them, may constitute a breach of professional boundaries and trust. This is particularly relevant where there is a perceived imbalance of power or influence arising from the staff members former position. Staff must not exploit their professional position to pursue or establish personal, social or otherwise inappropriate relationships with ex-pupils.

If any member of staff becomes aware that they themselves have been or another staff member has been speaking to a pupil or ex-pupil online, they should raise it to their line manager or Headteacher immediately.

Any failure to report concerns relating to safeguarding and social media may itself be treated as a disciplinary matter.

6.3. Use of emojis, GIF's and Memes

Using emojis, GIF's or memes can have their benefits, however it is important to use them correctly and appropriately.

You should be aware that messages and comments that include emojis may affect the way text is read. Emojis may mean different things to different people, the use of them may mean the text is deemed inappropriate.

If you choose to use emojis, GIF's or memes you should ensure they are appropriate and easily understood within the context.

6.4. Absence from work and use of social media

Use of social media whilst absent can create the impression that staff are well enough to be working. We accept that this is not necessarily the case, but this may be how it is perceived by colleagues and others. Taking this into account we would guide staff to be mindful of their use of social media during absence from work. Each case will be considered on its individual facts, and no assumptions will be made solely based on social media activity.

7. Guidelines for responsible use of social media

You should make it clear in social media postings that you are speaking on your own behalf.

You should be respectful to others when making any statement on social media and be aware that you are personally responsible for all communications which will be published on the internet for anyone to see. You should ensure that you use privacy and access settings whilst being aware that you cannot control the use of your postings by others.

All communication with pupils must take place through approved school systems.

You should also ensure any content you post on social media is consistent with the professional

image you present to colleagues, pupils, and parents.

If you are uncertain or concerned about the appropriateness of any statement or posting, you are advised to refrain from posting it until you have discussed it with your line manager.

Any contact with ex-pupils must be approached with professional judgement and transparency. Where there is any doubt about the appropriateness of contact, staff should seek advice from their line manager or the Designated Safeguarding Lead (DSL) before engaging.

If you become aware of social media content that disparages or reflects poorly on us, you should contact your line manager or Headteacher.

8. Monitoring

We reserve the right to monitor, intercept and review your use of social media. We consider valid reasons for checking your internet usage include suspicions that you have:

- been using social media when you should have been working.
- acted in a way that is in breach of the rules set out in this policy.

Monitoring is in our legitimate interests and is to ensure that this policy is being complied with. Monitoring will be proportionate, carried out in accordance with data protection legislation, and limited to what is necessary to achieve a legitimate purpose.

For further information, please refer to data security policy.

9. Breach of this policy

Any concerns or alleged breaches will be considered fairly and may be investigated in line with the School's disciplinary procedures. Breach of this policy may result in disciplinary action up to and including dismissal.

You may be required to remove any social media content that we consider to constitute a breach of this policy. Failure to comply with such a request may in itself result in disciplinary action.

Where this policy requires you to disclose matters from your personal life, we will consider the circumstances and context of each matter before determining whether any further action is required.

Appendix A – Online Safety Acceptable Use Agreement – Staff, Governors and student teachers (on placement or on staff)

You must read this agreement in conjunction with the online safety policy, the Data Protection policy, and the Data Security policy. Once you have read these, you must sign and submit this agreement and it will be kept on record in the school. You should retain your own copy for reference. This forms part of your professional and safeguarding responsibilities.

Internet, mobile and digital technologies are part of our daily working life, and this agreement is designed to ensure that all staff and governors are aware of their responsibilities in relation to their use. All staff, student teachers and governors are expected to adhere to this agreement and to the online safety policy. Any concerns or clarification should be discussed with the headteacher. Breaches will be investigated, recorded and, where appropriate, disciplinary procedures will apply, and police involvement will be sought.

Internet Access

I will not access or attempt to access any sites that contain any of the following: child abuse; pornography; discrimination of any kind; promotion of prejudice against any group; promotion of illegal acts; any other information which may be illegal or offensive. Inadvertent access on school equipment must be treated as an online safety incident, reported to the online safety lead and/or the DSP and an incident report completed.

Online conduct

I will ensure that my online activity, both in and outside school, will not bring the school, my professional reputation, or that of others, into disrepute.

I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory. Exceptionally, use of controversial material as part of the curriculum should be planned and approved on every occasion (see policy).

I will report any accidental access to or receipt of inappropriate materials or filtering breach to Louise Whitby.

I understand that all my use of the internet and other related technologies can be traced and monitored and, should it be required, must be made available to my line manager, headteacher and others as required.

I will not give out my personal contact and online account information such as phone numbers, email address, and social media account details to pupils and/or parents/carers.

Should I be a member of staff and parent I will not contact pupils at Giles junior school through my child's or own personal mobile device. Any concerns relating to online conduct between my child and his/her peers will be directed to be dealt with by SLT so there is no conflict of interest.

Social networking

I understand the need to separate my professional role from my private friendships; in my professional capacity I will not become 'friends' with parents/carers or pupils (present or past) on social networks. Where my school role is my only connection to an individual, private online contact is unacceptable with parents/carers or pupils.

When using social networking for personal use I will ensure my settings are not public. My private account postings will never undermine or disparage the school, its staff, governors, parents/carers or pupils. Privileged information must remain confidential.

I will not upload any material about or references to the school or its community on my personal social networks.

Passwords

I understand that there is no occasion when a password should be shared with a pupil or anyone who is not a staff member.

Data protection

I will follow requirements for data protection as outlined in the Data Protection policy. These include:

- Photographs must be kept securely 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
- **Any personal or sensitive data taken off site must be encrypted.**

Images and videos

I will only upload images or videos of staff, pupils or parents/carers onto school approved sites where specific permission has been granted.

I will not take images, sound recordings or videos of school events or activities on any personal device. There are school cameras and video cameras for such use if required.

Use of email

I will use my school email address or Google classroom for all school business. All such correspondence must be kept professional and is open to Subject Access Requests under the Freedom of Information Act and General Data Protection Regulations. I will not use my school email addresses or Classroom for personal matters or non-school business.

Use of personal devices

I understand that as a member of staff I should at no time put myself in a position where a safeguarding allegation can be made against me as a result of my use of personal devices. I understand that the use of personal devices in school is at the discretion of the headteacher.

I will only use approved personal devices in designated areas and never in front of pupils.

I will not access secure school information from personal devices when in school or any other location unless a closed, monitorable system has been set up by the school. Such a system would ensure as the user, I was not saving files locally to my own device and breaching data security.

A monitorable system would be one such as LARA. Through LARA any school documents accessed on a personal device are never actually on the computer being used, they remain on the school server. When the user logs-out of LARA, there are no copies left on their own device.

Additional hardware/software

I will not install any hardware or software on school equipment without the permission of Louise Whitby.

Use of AI

Neither staff nor pupils should use AI tools to generate, edit, or share content unless explicitly authorised within school policy. Any permitted use of AI must follow school guidance and never involve personal or pupil data.

Giles Junior School do not currently have a ratified policy on the use of AI within school. When this is implemented staff will be expected to adhere to it. Staff conduct online, including in private use of social media or AI tools, must not bring the school into disrepute or expose children to risk

Attendance

Attendance is a safeguarding issue. In line with statutory guidance *Working Together to Improve School Attendance*, staff must monitor and report patterns of absence promptly.

Promoting online safety

I understand that online safety is the responsibility of all staff and governors and I will promote positive online safety messages at all times including when setting homework or providing pastoral support.

I understand that it is my duty to support a whole school safeguarding approach and will report any inappropriate or concerning behaviour (of other staff, governors, visitors, pupils or parents/carers) to the DSP.

Classroom management of internet access

I will pre-check for appropriateness all internet sites used in the classroom; this will include the acceptability of other material visible, however briefly, on the site. **I will not free-surf the internet in front of pupils.** I will also check the appropriacy of any suggested sites suggested for home-learning.

If I am using the internet to teach about controversial issues I will secure, on every occasion, approval in advance for the material I plan to use with the headteacher.

Video conferencing

I will only use the conferencing tools that have been identified and risk assessed by the school leadership, DPO and DSP. A school owned device should be used when running video-conferences, where possible.

User signature

I agree to follow this Acceptable Use Agreement and to support online safety throughout the school. I understand this forms part of the terms and conditions set out in my contract of employment (staff members only) and/or my responsibilities as a governor.

Signature Date

Full Name (printed)

Job title

Appendix B - Acceptable Use Agreement - Peripatetic teachers/coaches and supply teachers

School - Giles Junior School

Online safety lead – Louise Whitby

Designated Safeguarding Lead (DSL) Louise Whitby

This agreement forms part of your professional and safeguarding responsibility in the school. You must read and sign this agreement. This will be kept on record, and you should retain your own copy for reference.

Internet, mobile and digital technologies are part of our daily working life, and this agreement is designed to ensure that all staff and governors are aware of their responsibilities in relation to their use. You are expected to adhere to this agreement. Any concerns or clarification should be discussed with the DSP. Breaches will be investigated, recorded and, where appropriate, disciplinary procedures will apply, and police involvement will be sought.

The school's online safety policy will provide further detailed information as required.

Internet Access

I will not access or attempt to access any sites that contain any of the following: child abuse; pornography; discrimination of any kind; promotion of prejudice against any group; promotion of illegal acts; any other information which may be illegal or offensive. Inadvertent access on school equipment must be treated as an online safety incident and reported to the DSP and an incident report completed.

Online conduct

I will ensure that my online activity, both in and outside school, will not bring the school, my professional reputation, or that of others, into disrepute.

I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory. Exceptionally, use of controversial material as part of the curriculum should be planned and approved on every occasion (see policy).

I will report any accidental access to or receipt of inappropriate materials or filtering breach to Louise Whitby.

I understand that all my use of the internet and other related technologies can be traced and monitored and, should it be required, must be made available to my line manager, headteacher and others as required.

I will not give out my personal contact and online account information such as phone numbers, email address, and social media account details to pupils and/or parents/carers.

Should I need to share my professional details, such as mobile phone number or email address, with parent/carers, this must be agreed in advance as an acceptable approach with Louise Whitby.

Should I be a member of staff and parent I will not contact pupils at Giles junior school through my child's or own personal mobile device. Any concerns relating to online conduct between my child and his/her peers will be directed to be dealt with by SLT so there is no conflict of interest.

Social networking

I understand the need to separate my professional role from my private friendships; in my professional capacity I will not become 'friends' with parents/carers or pupils on social networks. Where my school role is my only

connection to an individual, private online contact is unacceptable with parents/carers or pupils.

Information can be shared with pupils over 13 and parents/carers through an organisational social network site/page e.g. on Facebook or Twitter, but never through a personal account or site. In my professional role in the school, I will never engage in 1-1 exchanges with pupils or parent/carers on personal social network sites.

My private account postings will never undermine or disparage the school, its staff, governors, parents/carers or pupils. Privileged information known as a result of my work in the school must remain confidential.

I will not upload any material about or references to the school or its community on my personal social networks.

Passwords

I must clarify what access I may have to the internet and/or school systems. If I have access of any kind, I understand that I must protect my password and there is no occasion when a password should be shared with a pupil or anyone who is not a staff member.

Data protection

I will follow all requirements for data protection explained to me by the school. These include:

- I must consult with the school before making any recordings, photographs, and videos. Once agreed, these must be made on a school device.
- I understand that there are strict controls and requirements regarding the collection and use of personal data. I will follow all requirements regarding GDPR.

Images and videos

I will only upload images or videos of staff, pupils or parents/carers onto school approved sites where specific permission has been granted.

I will not take images, sound recordings or videos of tuition or wider school activities on any personal device. School devices can be used for this purpose or, in the case of 1:1 tuition, pupil's or parent/carer devices can be used, with parent/carer agreement.

Internet, mobile and digital technologies provide helpful recording functions, but these cannot be made on a teacher's personal device. Recordings can be made with the child's and parent/carer's agreement on a school device, an organisational device approved by the headteacher/DSL, or a young person's or parent/carer's own device.

Use of Email

I will only use my professional email address for all school business. All such correspondence should be kept professional and is open to Subject Access Requests under the Freedom of Information Act and GDPR. I will not use my professional email addresses for personal matters.

Use of personal devices

I understand that when working in the school I should at no time put myself in a position where a safeguarding allegation can be made against me as a result of my use of personal devices. I understand that the use of personal devices in school is at the discretion of the headteacher.

I will only use approved personal devices in designated areas and never in front of pupils. This therefore precludes use of specialist apps on personal devices. A school device could be used to access specialist apps that support pupil learning. Pupils can also be encouraged, but not required, to access such apps on their own devices if allowed by the school and with parent/carer agreement.

Additional hardware/software

I will not install any hardware or software on school equipment without permission of Louise Whitby.

Promoting online safety

I understand that online safety is part of my responsibility and I will promote positive online safety messages at all times, including when setting homework, rehearsal or skill practice or when providing pastoral support.

I understand that it is my duty to support a whole school safeguarding approach and will report any behaviour (of staff, governors, visitors, pupils or parents/carers) which I believe may be inappropriate or concerning in any way to the DSP.

Classroom management of internet access

I will pre-check for appropriateness all internet sites used in the classroom or during a tutoring session, this will include the acceptability of other material visible, however briefly, on the site. I will not free-surf the internet in front of pupils.

If I am using the internet to teach about controversial issues I will secure, on every occasion, approval in advance for the material I plan to use with the headteacher.

Video conferencing

I will only use the conferencing tools that have been identified and risk assessed by the school leadership, DPO and DSP. A school-owned device should be used when running video-conferences, where possible.

User Signature

I agree to follow this Acceptable Use Agreement and to support online safety in my work in the school. I understand this forms part of my company/educational setting/organisation's contract with the school.

Signature Date

Full Name (Please use block capitals)

Job Title/Role

Appendix C - Requirements for visitors, volunteers and parent/carers helpers working in the school (working directly with children or otherwise)

School - Giles Junior School

Online safety lead – Louise Whitby

Designated Safeguarding Lead (DSP) Louise Whitby

This document is designed to ensure that you are aware of your responsibilities when using any form of IT in the school and other aspects of safeguarding in connection with online safety.

Please raise **any** safeguarding concerns arising from your visit immediately with the headteacher and/or DSP

- I understand I may only use my personal mobile phone(s) and other devices with camera functions in designated areas. When not in a designated area, phones must be switched off and out of sight. Any exception must be pre-arranged.
- I will not take images, sound recording or videos of school events or activities, on or off site, on any device. Any possible exception must be pre-arranged.
- I will not give out my personal details such as mobile phone number, email address, and social media account details to pupils. Where appropriate I may share my professional contact details with parents/carers provided the DSP is informed before I leave the school.
- I understand my visit to the school may give me access to sensitive information about pupils, staff, school systems and plans. Such information should never be shared online, including on social media sites.
- I understand I should not use school equipment to access the internet without prior approval from my contact in the school or the headteacher.
- If working in the classroom, I will pre-check for appropriateness all internet sites I intend to use including checking the acceptability of other material visible on the site. I will not free-surf the internet in front of pupils. If I am in any doubt about the appropriateness of the content I plan to use I will check with my contact in the school.

Appendix D - Online Safety Acceptable Use Agreement Primary Pupils

My online safety rules

- I will only use school IT equipment for activities agreed by school staff.
- I will not use my personal email address or other personal accounts in school when doing school work.
- I will not sign up for any online service on school devices unless this is an agreed part of a school project approved by my teacher and agreed by my parent/carer.
- I will only open email attachments if it has been approved by a member of school staff in school or a parent/carer out of school.
- In school I will only open or delete my files when told by a member of staff.
- I will not tell anyone other than my parents/carers my passwords. I will not use other people's usernames or passwords to pretend to be them online.
- I will make sure that all online contact I make is responsible, polite, and sensible. I will be kind and respectful at all times.
- If I come across anything upsetting, unpleasant or nasty, or anything that makes me feel unsafe, I will tell my teacher or my parent/carer immediately.
- If someone says, asks or posts about me anything upsetting, unpleasant or nasty, or anything that makes me feel unsafe, **I will not reply**. I will tell my teacher or my parent/carer immediately.
- I will not give out my own or other people's personal information, including: name, phone number, home address, interests, schools or clubs. I will tell my teacher or parent/carer if anyone asks me online for personal information.
- Uploading or sending my image (photographs, videos, live streaming) online puts me at risk. I will always seek permission from my teacher or parent/carer if I wish to do this. I will not take, share or upload any image of anyone else without their permission and also, if they are a child, without their parent's/carer's permission.
- Even if I have permission, I will not upload any images, videos, sounds or words that **could** upset, now or in the future, any member of the school community, as this is cyberbullying.
- I understand that some people on the internet are not who they say they are, and some people are not safe to be in contact with. I will not arrange to meet someone I only know on the internet. If someone asks to meet me, I will not reply to them and I will tell a teacher or a parent/carer immediately.
- I understand that everything I do or receive online can be traced now and in the future. I know it is important to build a good online reputation.
- I understand that some personal devices are allowed in school, and some are not, and I will follow the rules. I will not assume that new devices can be brought into school without getting permission.
- I understand my behaviour in the virtual classroom should mirror that in the physical classroom.

- **I will not lie about my age in order to access games, apps or social networks that are for older people as this will put me at risk.**
- I understand that these rules are designed to keep me safe now and in the future. If I break the rules my teachers will look into it and may need to take action.

Dear Parent/Carer,

The internet, email, mobile technologies and online resources have become an important part of learning and life. We want all children to be safe and responsible when using any IT. It is essential that children are aware of online risk, know how to stay safe and know where to go to report problems or get help.

Please read through these online safety rules with your child/ren and talk with them to ensure they understand their importance and what it means for them (and for you). When you have done this, you both need to sign this agreement to say that you agree to follow the rules. Any concerns or explanation can be discussed with the head teacher – Louise Whitby.

Please return the signed sections of this form which will be kept on record at the school.

Pupil agreement

Pupil name.....

Pupil signature.....

This agreement is to keep me safe. I have discussed this agreement with my parents/carers and understand the commitment I have made and my responsibilities.

Parent(s)/Carer(s) agreement

Parent(s)/Carer(s) name(s).....

Parent/carers signature.....

Date.....

I/we have discussed this agreement, which highlights the associated risks when accessing the internet, mobile and digital technologies, with our child/ren. I/we agree to support them in following the terms of this agreement.

I/we also agree not to share school related information or images online or post material that may bring the school or any individual within it into disrepute.

(Rather than posting negative material online, any parent, distressed or concerned about an aspect of school should make immediate contact with a member of staff. Negative postings about the school would impact on the reputation of the whole school community. Parents are encouraged to report breaches so that we can protect the reputation of the school, staff, pupils, and parents).

I/we also agree only to use personal mobile phones and devices in designated areas of the school unless otherwise informed, e.g., for specific events and activities. I/we understand that under no circumstance should images be taken at any time on school premises of anyone other than our own child/ren, unless there is a pre-specified agreement. I/we understand that when on school premises, but not in a designated area where phones can be used, they must be switched off and out of sight.

Appendix E – Online safety policy guide – Summary of key parent/carers responsibilities

The school provides online safety information for parents/carers, through the website, in newsletters and at events. It is important that parents/carers understand their key role in supporting children to behave appropriately and keep themselves safe online.

The online safety policy, supported by its acceptable use agreements, is intended to protect the interests and safety of the whole school community.

- Parents/carers are required to support their child in understanding and signing the Online Safety Acceptable Use Agreement for pupils.
- Parents/carers may only use personal mobile phones and devices in designated areas of the school unless otherwise informed, e.g., for specific designated area, their phone/s must be switched off and out of sight. events and activities. Under no circumstance should images be taken at any time on school premises that include anyone other than their own child, unless there is a pre-specified agreement with individuals and parents/carers. When a parent/carer is on school premises but not in a designated area, their phone/s must be switched off and out of sight.
- Parents/carers should not assume that pupils can bring technological devices to school and should always check the school policy.
- All cyberbullying incidents affecting children in the school should be reported immediately. (If the incident involves an indecent image of a child the report must also be made immediately to the police for your own protection.) The school will investigate and respond to all reported cyberbullying incidents, liaising with others where appropriate. No reply should ever be sent to the sender/poster of cyberbullying content. If applicable block the sender and report abuse to the site. Evidence should be retained and shown in school and/or to the police. Evidence should not be forwarded.
- The school may choose to set up social media sites, blogs or have some other online presence in its own name. Parents/carers, however, do not have the right to set up any site, page, chat group or any other online presence that uses the school name or logo in any form.
- Any parent/carer, distressed or concerned about an aspect of school should make immediate contact with a member of staff rather than posting their concerns online. Parents/carers should not share school related information or images online or post material that may bring the school or any individual within it into disrepute. Negative postings about the school would impact on the reputation of the whole school community. Parents/carers are encouraged to report breaches so that we can protect the reputation of the school, staff, pupils and parents/carers.

Please see the full online safety policy in the policies section on the school website.

Appendix F - Guidance on the process for responding to cyberbullying incidents

All cyberbullying incidents should be reported and responded to. Cyberbullying usually happens in the family home or outside of school. The first point of contact should be for the child to report this to a trusted adult. We recommend the parent or carer follows the process stated below. If the parent or carer has been unable to resolve the issue and has concerns that the incident may affect relationships within school hours, then the school should be notified. Where the perpetrator is a member of the school community the majority of cases can be dealt with through mediation and/or disciplinary processes.

The following procedures are recommended:

- Never reply to the sender/poster of cyberbullying content. If applicable, block the sender.
- Incidents should be reported immediately. Pupils should report to a member of staff (e.g., class teacher, headteacher) and staff members should seek support from their line manager or a senior member of staff.
- Further parameters may be instilled in the family home if appropriate such as ensuring all interactions are held in a room which is public, rather than privately in a bedroom.
- The person reporting the cyberbullying should save the evidence and record the time and date. This evidence must not be forwarded but must be available to show at a meeting. Under no circumstances should indecent images of children and young people be printed or forwarded as this is a further criminal act. Staff should not ask to see the evidence of reported indecent images of children or young people but must refer this immediately to the police. Any member of staff being shown such evidence should immediately inform their line manager or the headteacher so that the circumstances can be recorded.
- Pupils, parents or carers who feel the incident has not been resolved should report to a member of staff. In the first instance this should be the child's teacher. The staff member should seek support from their line manager or a senior member of staff if they feel it is necessary.
- Should a senior member of staff be required then they will meet with the person who has reported the incident and the target, if different, to listen, reassure and support. All relevant facts will be reviewed and documented.
- A senior member of staff will conduct an investigation.
- Anyone found to have cyberbullied will have attention drawn to the seriousness of their behaviour and if necessary the police will be involved. If the comments are threatening, abusive, sexist, of a sexual nature, constitute a hate crime or are libellous they may well break the law. Online harassment and stalking is also a crime.
- Once evidence has been secured then the person who has cyberbullied will be requested to remove the offending comments/material. Any refusal will lead to an escalation of sanctions.

Appendix G - Guidance for staff on preventing and responding to negative comments on social media

The school should make it clear which, if any, social media platforms are used to communicate with parents/carers. If used correctly, parents can use a school's social media site as a source of reliable information. The online safety policy, see especially Appendix E (Online safety policy guide - Summary of key parent/carer responsibilities), clarifies that no other social media platforms should be set up using the school's name or logo.

The school should regularly reinforce with all parties that discussion of school issues on social media platforms, either positive or negative, should not take place as this could bring the school into disrepute and affect families and children. Parents should be encouraged to be good online role models and not post statements written in anger or frustration. Identified routes to raise concerns directly with the school should be used.

If negative comments are posted:

Collect the facts

As soon as you become aware of adverse comments relating to the school you need to establish what is being said. It is essential that if you have access to the postings they are secured and retained together with any other evidence. Do not become engaged in responding directly.

If the allegations against a member of staff or a pupil are of a serious nature, these will need to be formally investigated. This may involve the police and the headteacher will need to follow the school's safeguarding procedures.

If there is a risk of serious damage to the school reputation or the reputation of individual members of staff, professional legal advice should be sought.

Adverse comments of any kind are highly demotivating and cause stress and anxiety. It is important that the senior staff reassure and support all staff and/or other affected members of the school community.

Addressing negative comments and complaints

Contact the complainants and invite them to a meeting. In the meeting, make sure you have any evidence available.

The meeting must:

- Draw attention to the seriousness and impact of the actions/postings.
- Ask for the offending remarks to be removed.
- Explore the complainant's grievance.
- Agree next steps.
- Clarify the correct complaints procedures.

If the meeting does not resolve the issue, the parents must be informed that the school will need to take the matter further. This may include:

- Reporting the matter to the social network site if it breaches their rules or breaks the law.
- Reporting the matter to the police if it breaks the law, e.g., if the comments are threatening, abusive, malicious, sexist, of a sexual nature, constitute a hate crime or are libellous they may well break the law. Online harassment and stalking is also a crime.

If inappropriate postings continue or the original material is not removed, a second meeting is advisable to re-iterate the seriousness of the matter.

Appendix H – Safeguarding and remote education during coronavirus (COVID-19)

Useful resources

Below are resources (please note not an exhaustive list) to help schools manage and risk assess any remote teaching and working.

Government guidance on safeguarding and remote education

<https://www.gov.uk/guidance/safeguarding-and-remote-education-during-coronavirus-covid-19>

The Key for School Leaders- Remote learning: safeguarding pupils and staff

<https://schoolleaders.thekeysupport.com/covid-19/safeguard-and-support-pupils/safeguarding-while-teaching/remote-teaching-safeguarding-pupils-and-staff/?marker=content-body>

NSPCC Undertaking remote teaching safely

<https://learning.nspcc.org.uk/news/2020/march/undertaking-remote-teaching-safely>

LGfL Twenty safeguarding considerations for lesson livestreaming

<https://static.lgfl.net/LgflNet/downloads/digisafe/Safe-Lessons-by-Video-and-Livestream.pdf>

swgfl Remote working a guide for professionals

<https://swgfl.org.uk/assets/documents/educational-professionals-remote-working.pdf>

National Cyber Security Centre Video conferencing. Using services securely

https://www.ncsc.gov.uk/files/vtc_infographic.pdf

Any remote learning or video-conferencing must follow DfE's 2025 safeguarding guidance, using only school-approved platforms and devices, with risk assessments in place.