Elkesley Primary & Nursery School

Online Safety Policy

2024/2025

Compiled by	C Marsh	September 2024
Agreed by	Staff	September 2024
Approved by	Governing Body	September 2024
Signed		
To be reviewed September 2025		

Our staff are aware that technology offers many opportunities but is a significant component in many safeguarding and wellbeing issues. Children are at risk of abuse online as well as face to face. Children can also abuse their peers online, this can take the form of abusive, harassing, and misogynistic messages, the non-consensual sharing of indecent images, especially around chat groups, and the sharing of abusive images and pornography, to those who do not want to receive such content.

All our staff have 'an understanding of the expectations, applicable to their roles and responsibilities in relation to filtering and monitoring' of ICT systems and regular monitoring of school's equipment and networks.

Our school approach to online safety, including appropriate filtering and monitoring on school devices and school networks is reflected in this Child Protection Policy including awareness of the ease of access to mobile phone networks. (See KCSiE 2024)

Our Snr DSL and the DSL team has the lead responsibility in this area, which is overseen and regularly reviewed by the 'Governing body, along with considering the number of and age range of our children, those who are potentially at greater risk of harm, and how often they access the IT system along with the proportionality of costs versus safeguarding risks.'

Our *Governing body* will ensure they maintain oversight of *the Online Safety Policy*, and the arrangements put in place to ensure appropriate filtering and monitoring on school devices and school network. The appropriateness of any filtering and monitoring systems will in part be informed by the risk assessment required by the Prevent Duty as required by KCSiE 2024.

This will include:

- identify and assign roles and responsibilities to manage filtering and monitoring systems.
- review filtering and monitoring provision at least annually.
- block harmful and inappropriate content without unreasonably impacting teaching and learning.
- have effective monitoring strategies in place that meet the school/ colleges safeguarding need**.**
- review and discuss the standards with the leadership team, IT staff and service providers to ensure the school meets the standard published by the Department for Education filtering and monitoring standards.

Roles and Responsibilities

Governing body

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.
The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governor who oversees online safety is Louise Douglas Koch.

All governors will:

- Ensure that they have read and understand this policy
- Regularly reviewing Online Safety incidents.

- Ensuring Online Safety policies, procedures, responsibilities, technological tools and education programme are regularly reviewed as part of child protection and health and safety.
- Ensuring access to relevant training for all school staff.
- Supporting the Online Safety co-ordinator in the development of an e-safe culture
- Promoting Online Safety to parents and carers.

Headteacher

- The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.
- Developing, owning and promoting the Online Safety vision to all stakeholders.
- Supporting the Online Safety co-ordinator in the development of an e-safe culture.
- Making appropriate resources available to support the development of an e-safe culture.
- Receiving and regularly reviewing Online Safety incident logs.
- Regularly reviewing Online Safety policies, procedures, technological tools and education programmes as
- part of child protection and health and safety
- Supporting the Online Safety co-ordinator in the appropriate escalation of Online Safety incidents.
- Taking ultimate responsibility for Online Safety incidents.

The Designated Safeguarding Leads

Details of the school's DSL are set out in our child protection and safeguarding policy as well as relevant job descriptions.

The DSL takes lead responsibility for online safety in school, in particular:

- Ensure that staff understand this policy and that it is being implemented
- consistently throughout the school
- Working with SLT, computing lead and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school child protection policy
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school
- behaviour policy
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or governing board
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy.

IT Technician

Elkesley Primary and Nursery School's IT technician is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's IT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's IT systems on monthly basis

- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

Computing Lead
The Computing lead is responsible for:
- Developing an e-safey culture and acting as a named point of contact on all Online Safety issues.
- Ensuring that Online Safety is embedded within continuing professional development (CPD) for staff and coordinating training as appropriate.
- Ensuring that Online Safety is embedded across the curriculum (or other learning activities) as appropriate.
- Ensuring that Online Safety is promoted to parents and carers, and other users of network resources.
- Maintaining an Online Safety incident log.
- Monitoring and reporting on Online Safety issues to the management team, and other agencies as appropriate.
- Developing an understanding of the relevant legislation.
- Reviewing and updating Online Safety policies and procedures on a regular basis.

Teaching and support staff
All staff, including contractors and agency staff, and volunteers are responsible for:
- Contributing to the development of Online Safety policies.
- Maintaining an understanding of this policy
- Implementing this policy consistently
- Working with the DSL to ensure that any online safety incidents are logged on Myconcern appropriately in line with this policy
- Taking responsibility for the security of systems and data.
- Embedding Online Safety education in curriculum delivery wherever possible.
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with SEND because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable
- Identifying individuals of concern and taking appropriate action.
- Knowing when and how to escalate Online Safety issues.
- Maintaining a professional level of conduct in their personal use of technology, both within and outside school.
- Taking personal responsibility for their professional development in this area, including personal use of social media
- Maintaining a professional level of conduct in their personal use of technology and social media, both within and outside school and asking for support if needed
- Taking personal responsibility for their professional development in this area.
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

Parents and carers
Parents and carers are expected to:
- Discuss Online Safety issues with their children, supporting the school in its Online Safety approaches and reinforcing appropriate behaviours at home.
- Taking responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.
- Modelling appropriate uses of new and emerging technology.
- Liaising with school if they suspect, or have identified, that their child is conducting risky behaviour online.
- Notify a member of staff or the headteacher of any concerns or queries regarding this policy.

Risk and Harms

If we are to effectively safeguard our school communities, we must first understand where esafety risks and potential harms lie. Unfortunately, the breadth of the issues classified within
the term 'online safety' is considerable. Therefore, we have adopted the domains and definitions, as stated within key safeguarding guidance, (Keeping Children Safe in Education).

These '4 Cs' are listed as follows:

- **Content**: being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism.
- **Contact**: being subjected to harmful online interaction with other users; for example: peer to
  peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
- **Conduct**: personal online behaviour that increases the likelihood of, or causes harm; for example, making, sending, and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and or pornography, sharing other explicit images and online bullying.
- **Commerce**: risks such as online gambling, inappropriate advertising, phishing and or financial scams. Pupils or staff at risk can be reported to the Anti-Phishing Working Group

It is noted that where concerns pertain to sexualised harms are reported, staff are aware of the DfE searching screening and confiscation at schools guidance and Sharing nudes and seminudes: advice for education settings working with children and young people. The key consideration is for staff not to view or forward illegal images of a child.

Keeping Children Safe in Education has been updated to reflect the advances and emergence of wider e-safety harms and now makes specific reference to this issue. This relates to criminal activity committed using computers and/or the internet. It is broadly categorised as
either 'cyber-enabled' (crimes that happen off-line but are enabled at scale and at speed online) or 'cyber dependent' (crimes that can be committed only by using a computer).

Filtering and Monitoring

Elkesley Primary and Nursery School will manage the new filtering and monitoring requirements put in place by KCSiE 2024, by use a 'Smoothwall' firewall. All devices are connected to one school network which filters directly through firewall. Only approved sites can be accessed. Our IT technician ensures regular checks are made to ensure that filtering methods are effective; if staff or pupils discover an unsuitable site, it must be reported to the head teacher who will then record it and report to the IT technician; any material that the school suspects is illegal will be referred to the Internet Watch Foundation; emails are automatically filtered through use of office 365; All users have unique usernames to access the school network; virus protection is reviewed and updated regularly.

The filtering and monitoring provision is reviewed (at least annually) by senior leaders, the Designated Safeguarding Lead and a governor with the involvement of the IT Service Provider.

Filtering

Checks on the filtering system are carried out by the IT Service Provider with the involvement of a senior leader, the Designated Safeguarding Lead and a governor, in particular when a safeguarding risk is identified, there is a change in working practice.

There is a clear process in place to deal with, and log, requests/approvals for filtering changes; filtering logs are regularly reviewed and alert the Designated Safeguarding Lead to breaches of the filtering policy, which are then acted upon.

The school manages access to content across its systems for all users and on all devices using the schools internet provision. The filtering provided meets the standards defined in the DfE Filtering standards for schools and colleges and the guidance provided in the UK Safer Internet Centre Appropriate filtering. Smoothwall alerts are sent to the head teacher on a weekly basis with a date/time stamp, the type of content attempted to be accessed and the name of the site; along with the user who has attempted access.

Illegal content (e.g., child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation URL list and the police assessed list of unlawful terrorist content, produced on behalf of the Home Office. Content lists are regularly updated.

Monitoring

- There are established and effective routes for users to report inappropriate content, recognising that no system can be 100% effective.
- The school has monitoring systems in place to protect the school, systems and users:
- The school monitors all network use across all its devices and services.
- Monitoring reports are picked up, acted on and outcomes are recorded by the Designated Safeguarding Lead, all users are aware that the network (and devices) are monitored.
- There are effective protocols in place to report abuse/misuse. There is a clear process for prioritising response to alerts that require rapid safeguarding intervention. As soon as the teacher is alerted, the device is kept secure, the head/DSL is alerted to deal with the incident immediately and the concern is logged on MyConcern.
- Management of serious safeguarding alerts is consistent with safeguarding policy and practice.
- When using devices, children are reminded of expectations and are aware that spot checks of machines will be completed to ensure content searched for an accessed is in line with school policies.
- At the end of each session, 2 machines will be selected and checked to ensure content accessed is appropriate.
- Children are required to login with their own usernames to ensure their user is logged if inappropriate content is accessed.
- Along with this, children are to monitor content being accessed by classmates and are to ensure teachers are aware if any inappropriate content is being accessed.

Mobile Phones

Mobile phones are not permitted in school. If any child is to bring a mobile phone, for safeguarding reasons only, it is to be handed to the business manager as soon as the child arrives on site. It will then be kept securely until the end of the day.

Staff mobile phones are permitted onto school grounds although it is the responsibility of the staff member to ensure that there is no inappropriate content stored on their device when brought onto school grounds. It is clearly outlined in the staff Code Of Conduct that mobile phones for staff are only permitted at break times and in the school offices or staffroom.

Cyber-bullying

Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one

person or group by another person or group, where the relationship involves an imbalance of power.

Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be.

Class teachers will discuss cyber-bullying with their classes.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying.

This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

The school also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy.

Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

Staff Training/ CPD

- Staff are expected to complete e-safety training annually delivered by National Online Safety, for which they will receive a certificate and the computing lead will be notified of completion.
- All new staff will receive online safety training as part of their induction programme

Online Safety Curriculum

Online safety will be taught following the schools long term computing planning linked directly to PurpleMash and National Online Safety; online safety will also be taught through PSHE and via assemblies, whole school projects and online safety days.

In Key Stage 1, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

In Pupils in Key Stage 2 will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

By the end of primary school, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online

- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

The safe use of social media and the internet will also be covered in the computing and PSHCE curriculum where relevant.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

Support for Parents

Our Senior DSL and the DSL team will always act in the 'best interest of the child' and remain mindful of the importance with parents and carers about safeguarding concerns held for children and in particular children's access to online sites when away from school.
We will support understanding of harmful online challenges and hoaxes and share information with parents and carers and where they can get help and support.

Along with staff CPD and a taught curriculum for children, National Online Safety includes safeguarding guides for parents. The resources include Parents & Carers courses (presented by Myleene Klass), online video resources and weekly guides covering a huge range of topics, including: Online Relationships; Fake Profiles & Social Bots; Online Bullying; Online Grooming; Child Sexual Exploitation; Sexual Harassment & Violence; Sexting; Live Streaming; Online Identity; Screen Addiction and more.

The DSL holds an annual meeting for parents in staying safe online. This includes informing parents of the statistics and potential dangers; discussing potential scenarios; information on how to keep children safe.

School also distribute parents guides to new dangers including TikTok trends, Dangerous game content etc.

Further Information

Our Governing body will ensure a review is maintained to ensure the standards and discuss with IT staff and service providers these standards and whether more needs to be done to support our school in meeting and maintaining this standard and communicating these to staff, our pupils, parents, carers and visitors to the school who provide teaching to children as part of the learning and educational opportunities we provide.

If online abuse occurs, we will respond to it by:
- having clear and robust safeguarding procedures in place for responding to abuse (including online abuse)
- providing support and training for all staff and volunteers on dealing with all forms of abuse, including bullying/cyberbullying, emotional abuse, sexting, sexual abuse and sexual exploitation making sure our response takes the needs of the person experiencing abuse, any bystanders and our organisation as a whole into account

Acceptable Use Agreements

EYFS and KS1

This is how we stay safe when we use computers:
- I will ask a teacher or suitable adult if I want to use the computers/tablets
- I will only use activities that a teacher or suitable adult has told or allowed me to use
- I will take care of computers/tablets and other equipment
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong

- I will tell a teacher or suitable adult if I see something that upsets me on the screen
- I know that if I break the rules I might not be allowed to use a computer/tablet

KS2

When I use devices I must behave responsibly to help keep me and other users safe online and to look after the devices.

For my own personal safety:

- I understand that what I do online will be supervised and monitored and that I may not be allowed to use devices in school unless I follow these rules and use them responsibly
- I will keep my username and password safe and secure and not share it with anyone else
- I will be aware of "stranger danger" when I am online
- I will not share personal information about myself or others when online
- If I arrange to meet people off-line that I have communicated with online, I will do so in a public place and take a trusted adult with me
- I will immediately tell an adult if I see anything that makes me feel uncomfortable when I see it online.

I will look after the devices I use, so that the school and everyone there can be safe:

- I will handle all the devices carefully and only use them if I have permission.
- I will not try to alter the settings on any devices or try to install any software or programmes.
- I will tell an adult if a device is damaged or if anything else goes wrong.
- I will only use the devices to do things that I am allowed to do.

I will think about how my behaviour online might affect other people:

- When online, I will act as I expect others to act toward me.
- I will not copy anyone else's work or files without their permission.
- I will be polite and responsible when I communicate with others and I appreciate that others may have different opinions to me.
- I will not take or share images of anyone without their permission.

I know that there are other rules that I need to follow:

- I cannot use my own personal devices (mobile phones/USB devices etc.) in the school.
- Where work is protected by copyright, I will not try to download copies (including music and videos).
- When I am using the internet to find information, I should take care to check that the information is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.
- I should have permission if I use the original work of others in my own work.

I understand that I am responsible for my actions, both in and out of school:

- I know that I am expected to follow these rules in school and that I should behave in the same way when out of school as well.
- I understand that if I do not follow these rules, I may be subject to disciplinary action. This could include loss of access to the school network/internet, parents/carers contacted and in the event of illegal activities involvement of the police.

Teaching and support staff

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the

value of the use of digital technology for enhancing learning and will ensure that learners receive opportunities to gain from the use of digital technology.
I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of the school digital technology and communications systems.
- I understand that the rules set out in this agreement also apply to use of these technologies out of school, and to the transfer of personal data (digital or paper based) out of school
- I understand that the school digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules outlines in the code of conduct.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using school systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital/video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the school website) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use social networking sites in school in accordance with the Code of Conduct.
- I will only communicate with learners and parents/carers using official school systems such as ClassDojo. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school has the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my mobile devices in school, I will follow the rules set out in the Code Of Conduct.
- I will not use personal email addresses on the school's ICT systems.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email.
- I will ensure that my data is regularly backed up, in accordance with relevant school policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, terrorist or extremist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies.

- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School Personal Data Policy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted.
- Paper based documents containing personal data must be held in lockable storage.
- I understand that data protection policy requires that any staff or learner data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- When using the online systems in my professional capacity or for school sanctioned personal use:
- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).
- I understand that I am responsible for my actions in and out of the school:
- I understand that this acceptable use policy applies not only to my work and use of school's digital technology equipment in school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school
- I understand that if I fail to comply with this acceptable use agreement, I could be subject to disciplinary action.

Use of Social Media

Social media (e.g. Facebook, Twitter, LinkedIn) is a broad term for any kind of online platform which enables people to directly interact with each other. However, some games, for example Minecraft or World of Warcraft and video sharing platforms such as You Tube have social media elements to them.

The school recognises the numerous benefits and opportunities which a social media presence offers. Staff, parents/carers and learners are actively encouraged to find creative ways to use social media. However, there are some risks associated with social media use, especially around the issues of safeguarding, bullying and personal reputation.

School Accounts

Monitoring**:** School accounts must be monitored regularly and frequently (preferably 7 days a week, including during holidays). Any comments, queries or complaints made through those accounts must be responded to within 24 hours (or on the next working day if received at a weekend) even if the response is only to acknowledge receipt. Regular monitoring and intervention is essential in case a situation arises where bullying or any other inappropriate behaviour arises on a school social media account.

Behaviour: The school requires that all users using social media adhere to the standard of behaviour as set out in this policy and other relevant policies:

- Digital communications by staff must be professional and respectful at all times and in accordance with this policy. Staff will not use social media to infringe on the rights and privacy of others or make ill-considered comments or judgments about staff.
- School social media accounts must not be used for personal gain. Staff must ensure that confidentiality is maintained on social media even after they leave the employment of the school.
- Unacceptable conduct, (e.g. defamatory, discriminatory, offensive, harassing content or a breach of data protection, confidentiality, copyright) will be considered extremely

seriously by the school and will be reported as soon as possible to a relevant senior member of staff, and escalated where appropriate.
- When acting on behalf of the school, respond to harmful and / or offensive comments swiftly and with sensitivity.
- If a conversation turns and becomes offensive or unacceptable, school users should block, report or delete other users or their comments/posts and should inform the audience exactly why the action was taken

The tone of content published on social media should be appropriate to the audience, whilst retaining appropriate levels of professional standards. Key words to consider when composing online content are:

- Engaging
- Conversational
- Informative
- Professional

Use of images: School use of images can be assumed to be acceptable, providing the following guidelines are strictly adhered to.

- Permission to use any photos or video recordings should be sought in line with the school's digital and video images policy. If anyone, for any reason, asks not to be filmed or photographed then their wishes should be respected.
- Under no circumstances should staff share or upload learner pictures online other than via official school channels.
- Staff should exercise their professional judgement about whether an image is appropriate to share on school social media accounts. Learners should be appropriately dressed, not be subject to ridicule and must not be on any school list of children whose images must not be published.
- If a member of staff inadvertently takes a compromising picture which could be misconstrued or misused, they must delete it immediately.

Do:

- Check with a senior leader before publishing content that may have controversial implications for the school
- Use a disclaimer when expressing personal views
- Make it clear who is posting content
- Use an appropriate and professional tone
- Be respectful to all parties
- Ensure you have permission to 'share' other peoples' materials and acknowledge the author
- Express opinions but do so in a balanced and measured manner
- Think before responding to comments and, when in doubt, get a second opinion
- Seek advice and report any mistakes using the school's reporting process
- Consider turning off tagging people in images where possible
- Ensure the account is set up securely and the account can be transferred to another approved staff member in the event of the account holder leaving the school.

Don't:

- Don't make comments, post content or link to materials that will bring the school into disrepute
- Don't publish confidential or commercially sensitive material
- Don't breach copyright, data protection or other relevant legislation
- Don't link to, embed or add potentially inappropriate content. Consider the appropriateness of content for any audience of school accounts.
- Don't post derogatory, defamatory, offensive, harassing or discriminatory content
- Don't use social media to air internal grievances

Personal Accounts

- The use of social media by staff while at work may be monitored, and use in school is not permitted. Therefore, disciplinary action may be taken
- The school will take appropriate action in the event of breaches of the social media policy. Where conduct is found to be unacceptable, the school will deal with the matter internally. Where conduct is considered illegal, the school will report the matter to the police and other relevant external agencies, and may take action according to the disciplinary policy.
- Users of social media should consider the copyright of the content they are sharing and, where necessary, should seek permission from the copyright holder before sharing.
- Users must ensure that their use of social media does not infringe upon relevant data protection laws, or breach confidentiality.
- If you feel that you or someone else is subject to abuse by colleagues through use of online communications, then this action must be reported using the agreed school protocols.
- Personal communications are those made via a personal online accounts. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy.
- Personal communications which do not refer to or impact upon the school are outside the scope of this policy.
- Where excessive or inappropriate personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken.