

NANTWICH PRIMARY ACADEMY & NURSERY

PRINCIPAL – SUE SPENCE

Online Safety Policy



PAGE: 1 of 21 ISSUE: Eight DATE: September 2026 REVIEW: September 2027

Approved by: Susan Spence (Principal)
--

Nantwich Primary Academy & Nursery
Manor Road, Nantwich, Cheshire, CW5 5LX Tel
– 01270 902055
admin@nantwichprimaryacademy.co.uk

Online Safety Policy

Scope of the Policy

Online Safety encompasses the use of new technologies, internet and electronic communications such as mobile phones, collaboration tools and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience. The policy will operate in conjunction with other policies including those for student Behaviour, Anti-Bullying, Curriculum, Data Protection and Safeguarding. This policy applies to all members of the academy community (including staff, pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of academy ICT systems, both in and out of the academy.

What is Online Safety?

Online Safety encompasses the use of new technologies, internet and electronic communications such as mobile phones, collaboration tools and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

End to End Online Safety

Online Safety depends on effective practice at a number of levels:

Responsible ICT use by all staff and students, encouraged by education and made explicit through published policies.

Sound implementation of Online Safety policy in both administration and curriculum, including secure school network design and use.

Safe and secure broadband through Schools Broadband, with Lightspeed filtering and monitoring.

National Education Network standards and specifications.

Legislation and Statutory Guidance

This policy is based on the Department for Education's statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on preventing and tackling bullying and searching, screening and confiscation. It also refers to the Department's guidance on protecting children from radicalisation. It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so. The policy also takes into account the National Curriculum computing programmes of study.

It is the duty of the school to ensure that every child and young person in its care is safe. The same 'staying safe' outcomes and principles outlined in the Every Child Matters agenda apply equally to the 'virtual' or digital world.

Keeping Children Safe in Education 2026 sets out the legal duties that schools must follow to safeguard and promote the welfare of children and young people under the age of 18, including requirements relating to online safety. This expectation also applies to any voluntary, statutory and community organisations that make use of the school's ICT facilities and digital technologies.

Intent

To ensure that all members of our academy community understand and are committed to promoting respectful and responsible internet use.

To ensure that staff and pupils are aware of the benefits and risks associated with internet use and the use of social media.

To ensure that all necessary measures are in place to safeguard all.

To ensure that pupils feel safe and secure and are aware of how to keep themselves safe online.

To ensure that all members are aware of their responsibilities to safeguard themselves and others when accessing the internet and engaging in online activities.

Reviewing the Online Safety policy

The Online Safety Policy relates to other policies including those for ICT, bullying and child protection (safeguarding). The Computing curriculum coordinator will also act as Online Safety coordinator. The Online Safety Policy and its implementation will be reviewed at least annually, and sooner following significant changes to technology, safeguarding guidance, filtering and monitoring provision or emerging risk.

Teaching and learning

Technology is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils with quality Internet access as part of their learning experience.

In 2023 the school began its move to 1:1 iPad implementation with the children in KS2 and shared class set in KS1. The iPad is a tool for teaching and learning. Through the use of selected apps the staff can monitor the individual use of each iPad in their class. Through the app they can also safely navigate and lock children in and out of a variety of apps and websites. Staff are also aware that, if needed, they can lock iPads in order to check history and usage of each individual pupil. The use of appropriate apps e.g. Showbie and Jamf will further enhance our monitoring and ESafety procedures.

Keeping children safe using iPads

Staff are aware that the iPad is a tool to enhance teaching and learning through feedback and creativity.

Staff understand that too much screen time is not good for the children.

Jamf is managed centrally by the SBMAT IT Support Team, with the Computing Lead (Mr L. Bebbington) retaining academy-level administrator access to support device management and monitoring.

Internet safety filters applied to all pupil iPads.

Staff to receive training on use of Apple Classroom which displays a live feed of children's screens to ensure safe use.

Staff to 'Navigate' and 'Lock' pupil iPads when appropriate.

If children do misuse the iPad, they will receive a ban (based on severity of incident) and alternative resources to be made available in the classroom.

Technical support and central device-management support are provided by the SBMAT IT Support Team.

Pupil iPads are not currently taken home. Any future home-use arrangement would require prior SLT and SBMAT IT approval, a parent/carer agreement and clear expectations for responsible use.

Why are new technologies and Internet use important?

The internet is an essential element in 21st century life for education, business and social interaction.

The academy has a duty to provide students with quality internet access as part of their learning experience.

Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

The purpose of internet use in school is to raise educational standards, to promote pupil achievement and to support the professional work of staff.

Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

The school has a duty to provide students with quality Internet access as part of their learning experience.

Pupils use the Internet widely outside of school and will need to learn how to evaluate internet information and to take responsibility for their own safety and security.

Internet use will enhance learning

The school Internet access will be designed expressly for pupil use and will include internet usage monitoring and web filtering appropriate to the age of pupils.

Pupils will be taught what Internet use is acceptable and what is not and will be given clear objectives for Internet use.

Internet access will be planned to enrich and extend learning activities and to raise attainment and achievement. Access levels will be reviewed to reflect the curriculum requirements and age of pupils.

Staff should guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity.

Pupils will be educated in the effective use of the Internet in research, including the skills of effective knowledge location, retrieval and evaluation.

Pupils will be taught how to evaluate Internet content.

The academy will ensure that the copying and subsequent use of Internet derived materials by staff and pupils complies with copyright law.

Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Pupils will be Taught How to Stay Safe Online

At Nantwich Primary Academy, we educate our very youngest learners about the importance of online safety as we recognise that pupils are accessing an online world both in the home and school environment.

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.

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.

The safe use of social media and the internet will also be covered in other subjects where relevant. The academy will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

Cyber-Bullying

The rapid development of and widespread access to technology has provided a new medium for 'virtual bullying', which can occur in and outside school. Cyber-bullying is a different form of bullying which can happen beyond the school day into home and private space, with a potentially bigger audience, and more accessories as people forward on content. The importance of respectful online communications is explicitly taught and all pupils and parents are aware of our expectations.

The school will take all reasonable precautions to ensure against cyber-bullying whilst pupils are in its care. However, due to the global and connected nature of new technologies, it is not possible to guarantee that inappropriate use via a school computer will not occur. Neither the school, nor St. Bart's Multi-Academy Trust nor Cheshire East, can accept liability for inappropriate use, or any consequences resulting outside of school.

The school will proactively engage with pupils in preventing cyber-bullying by: Understanding and talking about cyber-bullying, e.g. inappropriate use of e-mail, text messages;

Keeping existing policies and practices up-to-date with new technologies;

Ensuring easy and comfortable procedures for reporting;

Promoting the positive use of technology;

Evaluating the impact of prevention activities.

Pupils, parents, staff and governors will all be made aware of the consequences of cyber-bullying.

Parents will be provided with an opportunity to find out more about cyber-bullying through: session for parents, NSPCC support guidance, and other outside agency support.

How will cyber-bullying reports/issues be handled?

Records of any incidents of cyber-bullying will be kept and will be used to help to monitor the effectiveness of the school's prevention activities. The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990. Methods to identify, assess and minimise risk will be reviewed regularly.

Complaints of cyber-bullying will be dealt with by a senior member of staff.

Any complaint about staff misuse must be referred to the Principal, or in the event a complaint is made of misuse by the Principal to the Chair of Governors and Link Governor for Safeguarding. Evidence of offending messages, pictures or online conversations will be kept, in order to demonstrate to others what is happening. It can be used by the school, internet service provider, mobile phone company, or the police, to investigate the cyber-bullying.

Pupils and parents will be informed of the complaints procedure.

Parents and pupils will need to work in partnership with staff to resolve issues.

Sanctions within the school discipline policy include:

Interview/reflection by the class teacher;

Informing parents or carers;

Removal of Internet/computer access for a period of time or banning of mobile phones in school (Year 6)

Prevent: Radicalisation and Extremism

Nantwich Primary Academy takes an active role in protecting pupils from the risks of extremism and radicalisation. Keeping children safe from risks posed by terrorist exploitation of social media is approached in the same way as safeguarding children from any other online abuse. In the same way teachers are vigilant about signs of possible physical or emotional abuse, we are vigilant about any signs of radicalisation or extremism in any of our pupils. We follow the same safeguarding procedure to ensure all children in our care are well looked after.

For more information on Prevent, Radicalisation and Extremism please follow the link on our website on the Child Protection and Safeguarding page.

Managing Internet Access Information system security.

School ICT systems capacity and security will be reviewed regularly. Virus protection will be updated regularly.

Security strategies will be discussed within Saint Bart's Trust.

E-mail

(In use if Teacher requests e.g. covering within the curriculum)

Pupils may only use approved e-mail accounts/messaging systems on the chosen school system. Pupils must immediately tell a teacher if they receive offensive e-mail or messages.

Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.

E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.

Published content and the school learning platform

The contact details on the Web site must be the school address, e-mail and telephone number.

Staff or pupils' personal information will not be published.

Publishing pupils' images and work

Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified. (No children's names to be used).

Pupils' full names will not be used anywhere on the Web site, particularly in association with photographs.

Written permission from parents or carers will be obtained before photographs of pupils or pupils' work are published on the school Web site. This is done on entry to school.

Social networking and personal publishing

The school will block/filter access to social networking sites. Newsgroups will be blocked unless a specific use is approved.

Pupils will be advised never to give out personal details of any kind which may identify them or their location.

Managing filtering

The school works with the SBMAT IT Support Team, Schools Broadband and Lightspeed to ensure filtering and monitoring systems are reviewed, maintained and improved.

If staff or pupils discover unsuitable content, or believe a site should be blocked or allowed, this must be reported through the academy's Online Safety / safeguarding route. Filtering decisions and technical changes are referred to and implemented by the SBMAT IT Support Team.

The Computing Lead, DSL and SBMAT IT Support Team work together to review the effectiveness of filtering and monitoring. The DSL receives daily Lightspeed monitoring updates and safeguarding concerns are escalated through the established safeguarding route.

Managing emerging technologies

Emerging technologies will be examined for educational benefit and safeguarding risk before use in school. This includes generative AI tools, unsupervised chatbots, AI-generated content and deepfakes. Staff and pupils will be supported to consider accuracy, privacy, age-appropriateness, bias, manipulation and the risk of harmful or misleading content.

Any new technology that processes personal data or presents a material safeguarding risk will be considered in line with relevant SBMAT data protection, safeguarding and acceptable use requirements.

Managing remote teaching/video-conferencing, the equipment and network

Remote teaching, video-conferencing and online meetings must use school-approved platforms and accounts. Sessions involving pupils will be supervised appropriately for their age and purpose, and staff will follow safeguarding, data protection and acceptable use requirements.

Only authorised staff will create or manage school meeting links or accounts. Meeting details must not be published publicly. Any recording must have a clear educational purpose, appropriate permission and secure storage.

Third-party content and external participants must be checked for suitability before use with pupils.

Content

When an online lesson, meeting or video-conference is recorded, participants must be informed. Recordings must have a clear purpose, use appropriate permissions, and be stored and shared securely in accordance with school and Trust policy.

Staff must check that third-party materials, external speakers and shared online content are appropriate for the pupils involved and do not breach copyright, confidentiality or data protection requirements.

Pupils using devices for home learning

Pupil iPads are not currently taken off school premises for home learning. If a future home-use arrangement is authorised, it will require SLT and SBMAT IT approval, appropriate Jamf management, a parent/carers agreement and clear responsible-use expectations.

The SBMAT IT Support Team manages Jamf centrally. The Computing Lead (Mr L. Bebbington) also retains academy-level Jamf administrator access to support day-to-day device management in school.

Any future home-learning arrangement will follow the SBMAT Acceptable Use Policy and relevant remote-learning, safeguarding and data-protection requirements.

Protecting personal data

Personal data will be recorded, processed, transferred and made available in accordance with the Data Protection Act 2018, UK GDPR and relevant SBMAT data-protection policies. Appropriate privacy notices and Data Protection Impact Assessments will be used where required, including for monitoring systems and new technologies.

Policy decisions

The Computing / Online Safety Lead will ensure staff can access the relevant academy and SBMAT policies and know the appropriate routes for reporting online-safety concerns.

Authorising Internet access

All staff must read and adhere to the acceptable use policy before using any school ICT resource.

Access to the Internet will be by supervised access to specific, approved on-line materials.

All staff must read and understand the related computing policies (see Related policies).

Assessing risks

The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor local authority can accept liability for the material accessed, or any consequences of Internet access. If unsuitable material appears, the Online Safety Lead & SLT will be informed so that relevant filtering can be completed.

The school will audit ICT provision to establish if the Online Safety policy is adequate and that its implementation is effective.

Handling Online Safety complaints

Complaints of Internet misuse will be dealt with by the class teacher and where necessary a senior member of staff.

Any complaint about staff misuse must be referred to the Principal.

Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

Pupils and parents will be informed of the complaints procedure.

Parents and pupils are expected to work in partnership with staff to resolve issues or concerns.

Sanctions within the school behaviour policy will include:

- interview/reflection by Learning Mentor/SLT;
- informing parents or carers;
- removal or restriction of Internet or computer access for a period.

Discussions will be held with the appropriate Police service to establish procedures for handling potentially illegal issues.

Community use of the Internet

In the event that external organisations are able to use the school's ICT facilities they must adhere to the Online Safety policy. Internet use by staff and children is actively monitored.

Communicating the Online Safety Policy

Introducing the Online Safety policy to pupils

Online Safety rules (SMART rules) will be posted in all networked rooms and discussed with the pupils at the start of each year and throughout the year as part of computing and PHSE sessions.

Pupils will be informed that network and Internet use will be monitored.

An Online Safety training programme will be introduced to raise the awareness and the importance of safe and responsible internet use.

Instruction in responsible and safe use should precede Internet access.

An Online Safety module will be included in the PSHE and Computing programmes covering both school and home use.

Staff and the Online Safety policy

All staff will be given the School Online Safety Policy and its application and importance explained.

All staff will be informed that all computer and Internet use will be monitored. Discretion and professional conduct is essential.

Staff training in safe and responsible Internet use and on the school Online Safety Policy will be provided as required.

Staff that manage filtering systems or monitor ICT use will be supervised by senior management and have clear procedures for reporting issues.

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation. In addition, all staff members will revisit or review this training as part of our annual safeguarding updates.

Enlisting parents' support

Parents' attention will be drawn to the school's Online Safety Policy in relevant newsletters, prospectus, the school website and through parent workshops / school event days. It is planned to produce a termly Online Safety newsletter.

A guide to Responsible Internet Use is also available on the school website.

Internet issues will be handled sensitively, and parents will be advised accordingly.

A partnership approach with parents will be encouraged. This could include parent evenings with demonstrations and suggestions for safe home Internet use.

Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be made available to parents.

Online Safety updates will be shared on both Class Dojo and other school social media to keep parents updated on relevant information.

Mobile Technology Device Policy

All devices that have access to a) the internet and b) the school network must be password protected. The purpose of this is to prevent data loss and protect pupils and staff.

Staff passwords

Staff each have their own username and unique password.

Staff generate their own password and understand that they must not share passwords. Records of staff passwords are not stored but the passwords can be overwritten or reset by the network administrator. Staff are expected to change their passwords at least annually to ensure that they remain secure.

Staff with access to sensitive data change their passwords regularly e.g. every term.

Pupil passwords

Each pupil has their own username and password for use on online learning platforms and other sign-in software.

Staff to record the pupil use of desktops / laptops and iPads in order to track any un-safe behaviour online or misuse of ICT software and equipment.

USB device password

USB devices are encrypted and password protected. The encryption password is chosen by the staff member but provided to admin for safe-keeping and safeguarding.

Hard drive encryption password

Laptop hard drives are encrypted and password protected. The encryption password is chosen by staff and shared only to those other staff members who require access to the laptop.

Please also refer to SBMAT Acceptable Use Policy; Learners and Staff

Personal mobile devices – staff and visitors

Staff and visitors are not permitted to make/receive calls/texts during contact time with children. Emergency contact should be made via the school office.

Staff and visitors should have their devices on silent or switched off and out of sight (e.g. in a drawer, handbag) during class time.

Mobile phones should not be used in a space where children are present (e.g. classroom, playground).

Use of devices (including receiving/sending texts and emails) should be limited to non-contact time when no children are present e.g. in office areas, staff room, empty classrooms.

Staff and visitors are not permitted to take photos or recordings or use any recording software with their personal devices without the explicit permission of the Principal.

Staff personal devices should use mobile data rather than school Wi-Fi; any device using school Wi-Fi is filtered.

Should there be exceptional circumstances (e.g. acutely sick relative), then staff and visitors should make the Principal and office staff aware of this so messages can be relayed promptly.

Staff and visitors should report any usage of mobile devices that causes them concern to the Principal.

All staff and visitors must password protect their mobile device.

Personal mobile devices – pupils

Pupils to only have phones when permission is granted from the school and parents in circumstances such as Year 6 children walking home alone.

Phones must be switched off during the school day.

Emergency contact to be made through the school office

Children are not permitted to take photos or recordings or use any recording software with their personal devices.

Any personal pupil device connected to the school network is subject to the same filtering controls.

School owned mobile devices – staff

All mobile devices including USB sticks must be password protected to prevent data loss

All mobile devices must be protected by the school's web filtering system

Passwords to devices must not be shared with anyone who is not employed by the school.

School owned mobile devices – pupils

All mobile devices must be protected by the school's web filtering system

Devices intended for pupil use must not leave the school

Pupils must access mobile devices using pupil user accounts only

Pupil mobile device user accounts must block any attempted file downloads, block access to the computer's system files, block access to the control panel, block access to the command prompt and only map the student network drive.

Miscellaneous

Wi-Fi access is restricted to authorised staff; a separate filtered guest login is available.

Related policies & Documents

There are a number of other policies at Nantwich Primary Academy which relate to the topics mentioned above. It is important that you read and fully understand the policies below which can be found on the school website or internal staff share file system. If you have any questions about this policy or any other policies relating to online safety please ask Mr Bebbington.

Social Media Policy

Social media (e.g. Facebook, Twitter, Tik Tok, 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 pupils/students 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. This policy aims to encourage the safe use of social media by the school, its staff, parents, carers and children.

Scope

This policy:

Applies to all staff and to all online communications which directly or indirectly, represent the school.

Applies to such online communications posted at any time and from anywhere.

Encourages the safe and responsible use of social media through training and education

Defines the monitoring of public social media activity pertaining to the school

The school respects privacy and understands that staff and pupils/students may use social media forums in their private lives. However, personal communications likely to have a negative impact on professional standards and/or the school's reputation are within the scope of this policy.

Professional communications are those made through official channels, posted on a school account or using the school name. All professional communications are within the scope of this policy.

Personal communications are those made via a personal social media 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.

Organisational control Roles & Responsibilities

SLT

Facilitating training and guidance on Social Media use.

Developing and implementing the Social Media policy

Taking a lead role in investigating any reported incidents.

Making an initial assessment when an incident is reported and involving appropriate staff and external agencies as required.

Staff

Know the contents of and ensure that any use of social media is carried out in line with this and other relevant policies

Attending appropriate training

Regularly monitoring, updating and managing content he/she has posted via school accounts

Adding an appropriate disclaimer to personal accounts when naming the school

Plan, and deliver lessons using 'Progression in Online Safety' from the NCCE computing SoW and national Online Safety organisations supplement this crucial learning.

Teach online safety as part of PHSE lessons.

Managing accounts

Process for creating new accounts

The school community is encouraged to consider if a social media account will help them in their work, e.g. a history department Twitter account, or a "Friends of the school" Facebook page. Anyone wishing to create such an account must present a business case to the School Leadership Team which covers the following points: The aim of the account
The intended audience

How the account will be promoted

Who will run the account (at least two staff members should be named)

Will the account be open or private/closed

Following consideration by the SLT an application will be approved or rejected. In all cases, the SLT must be satisfied that anyone running a social media account on behalf of the school has read and understood this policy and received appropriate training. This also applies to anyone who is not directly employed by the school, including volunteers or parents.

Monitoring

School accounts must be monitored regularly and frequently. Any comments, queries or complaints made through those accounts should 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.

If a journalist makes contact about posts made using social media staff must follow the school media policy before responding.

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.

The use of personal social media by staff while at work is prohibited.

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.

Legal considerations

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.

Handling abuse

When acting on behalf of the school, handle 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

If you feel that you or someone else is subject to abuse by colleagues through use of a social networking site, then this action must be reported using the agreed school protocols.

Tone

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 messages are: Engaging Conversational

Informative

Friendly (on certain platforms, e.g. Twitter) 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 student pictures online other than via school owned social media accounts

Staff should exercise their professional judgement about whether an image is appropriate to share on school social media accounts. Students 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.

Personal use

Staff

Personal communications are those made via a personal social media 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 personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken

The school permits reasonable and appropriate access to private social media sites.

Pupil/Students

Staff are not permitted to follow or engage with current or prior pupils/students of the school on any personal social media network account.

The school's education programme should enable the pupils/students to be safe and responsible users of social media.

Pupils/students are encouraged to comment or post appropriately about the school. Any offensive or inappropriate comments will be resolved by the use of the school's behaviour policy

Monitoring posts about the school

As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the school.

Managing your personal use of Social Media:

"Nothing" on social media is truly private

Social media can blur the lines between your professional and private life. Don't use the school logo and/or branding on personal accounts

Check your settings regularly and test your privacy

Keep an eye on your digital footprint

Keep your personal information private

Regularly review your connections – keep them to those you want to be connected to

When posting online consider; Scale, Audience and Permanency of what you post

If you want to criticise, do it politely.

Take control of your images – do you want to be tagged in an image? What would children or parents say about you if they could see your images?

Know how to report a problem?

Managing school social media accounts The Do's

Check with a senior leader before publishing content that may have controversial implications for the school

Use a disclaimer when expressing personal views

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

The Don'ts

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

Consider the appropriateness of content for any audience of school accounts, and don't link to, embed or add potentially inappropriate content

Don't post derogatory, defamatory, offensive, harassing or discriminatory content Don't

use social media to air internal grievances

Nantwich Primary Academy Internet Filtering Policy

Filtering and monitoring provision

All internet use on the school network is filtered. Nantwich Primary Academy uses Schools Broadband together with Lightspeed filtering and monitoring. Technical configuration, filtering decisions and changes are managed centrally by the SBMAT IT Support Team.

Network access

School Wi-Fi access is restricted to authorised users. A separate guest Wi-Fi login is available and is filtered. Staff personal mobile devices should normally use their own mobile data rather than school Wi-Fi. Any device connected to the school network is subject to the school's filtering controls.

Connecting a new device

School-managed devices are connected and configured through the academy and SBMAT IT management arrangements. Pupil iPads are managed through Jamf by the SBMAT IT Support Team, with academy-level administrator access also held by the Computing Lead.

Filtering profiles

Filtering is applied according to user and device type, with appropriate differentiated access for staff and pupils. Pupil filtering is more restrictive while still allowing access to appropriate educational content. Filtering also applies to guest devices using the school network.

Block / allow decisions

Staff who identify unsuitable content, or who require legitimate access to blocked content, should report this through the academy's Online Safety / safeguarding route. The SBMAT IT Support Team makes and implements filtering decisions or changes, taking account of safeguarding and educational need. Decisions and exceptions are controlled through the Trust's filtering management processes.

Safety and bypass protection

Schools Broadband and Lightspeed filtering are maintained centrally. Provider-managed illegal-content blocklists, including IWF and CTIRU lists, are applied. Filtering controls are configured to restrict attempts to bypass protection, such as through VPN or proxy services, without unreasonably restricting teaching and learning.

Monitoring and reporting

Lightspeed technical monitoring is active on school-managed devices. The DSL receives daily Lightspeed monitoring updates highlighting incidents. High-risk safeguarding concerns are escalated through the established DSL safeguarding route, with the SBMAT IT Support Team providing technical oversight and configuration.

Reports and monitoring information may be reviewed in more detail where required. Incidents, actions and outcomes are recorded through the academy's safeguarding procedures.

Review

Filtering and monitoring provision is reviewed at least annually and whenever significant changes, incidents or new risks arise. Review and assurance involve SLT, the DSL, SBMAT IT Support and responsible governance oversight.