



Contents

Contents.....	2
Objective.....	3
Scope.....	3
Introduction.....	3
Background.....	3
Business Use of Social media.....	4
Using Social Hubs.....	5
Personal Use of Social Media in the Workplace.....	5
No Expectation of Privacy.....	6
Guidelines for employees and Volunteers on the responsible use of Social Media.....	7
Safeguarding Issues.....	8
Recommendations.....	9
Compliance with this Policy.....	10
Frequently asked Questions.....	10
Linked Documents.....	16
Modification History.....	16

Objective

This policy is intended for the guidance of all employees and volunteers working on behalf of Nord Anglia Education whether based in a school or a central service. Nord Anglia Education encourages the use of social media to promote and celebrate the success of its students and staff, but wishes to ensure that employees and volunteers understand the potential implications when this form of communication is misused. The policy aims to explain the responsibilities and obligations to be considered when using social media and to provide simple guidance on some of these considerations.

Scope

This policy applies to all schools, entities and businesses in the Nord Anglia Education Group. It covers the use of social media in the workplace but also the personal use of social media, where personal communication could impact negatively on Nord Anglia Education. The policy will also apply to partner agencies and contractors working on behalf of Nord Anglia Education or on any Nord Anglia site.

In this policy, 'social media' refers to public and private posts, blogs, podcasts, wikis, video, social networks, and all emerging and as-yet-undiscovered social technologies.

Introduction

If used thoughtfully, social media is a powerful tool to engage our students, parents and communities. Nord Anglia Education encourages our schools to actively use social media channels to raise awareness, share information and celebrate their activities and successes.

We therefore encourage all staff and volunteers to 'think before you post' and follow Nord Anglia Education's General code of conduct and the safeguarding guidance for safer working practice when engaging with others on the internet and other forms of electronic communication.

Employees should only use social media on behalf of the organisation or any of our schools with permission and guidance from their school's Marketing, Admissions and Communications team or Nord Anglia Education's Central Marketing, Admissions and Communications team.

Background

The use of social networking sites such as Facebook, Snapchat and WhatsApp has rapidly become one of the primary forms of communication between friends, family and peers. In addition, there are many other sites which allow people to publish their own pictures, text and videos such as YouTube and blogging sites.

It would not be reasonable to expect or instruct employees not to use these sites which, if used with caution, should have no negative impact whatsoever on their role in school. Indeed, appropriate use of some sites may also have positive professional benefits.

It is naïve and out-dated, however, to believe that use of such sites provides a completely private platform for personal communications. Even when utilised sensibly and with caution employees are vulnerable to their personal details being exposed to a wider audience than they might otherwise have intended. One example of this is when photographs and comments are published by others without the employees consent or knowledge which may portray the employee in a manner not conducive to their role in school.

Difficulties arise when staff utilise these sites and do not have the knowledge or skills to ensure adequate security and privacy settings. They post inappropriate comments about another member of staff which they believe to be secure but which can actually be accessed by a much wider audience than initially intended. In addition, there are some cases where employees deliberately use these sites to communicate with and/or form inappropriate relationships with children and young people and/ or their families.

Business Use of Social Media

No employee should proactively or reactively use any form of social media on behalf of their school or Nord Anglia Education for marketing, public relations, or corporate communications without obtaining permission from the school principal and/or the admissions and marketing team, or from Nord Anglia Education's Central Marketing and Admissions team.

Similarly, if any employee is contacted by any social media outlet/provider and asked for comment about Nord Anglia Education or any of our schools, global projects and initiatives, you must direct the enquiry to Nord Anglia Education's Head of Brand. Please refer to the Media Relations policy for more details.

If you are given permission to use social media to share insights, stories, videos or photos from your school, you must follow the guidance provided by your school in doing this.

You will be effectively publishing / posting on behalf of Nord Anglia Education and our family of schools. In addition to the guidelines for responsible posting, please bear in mind the following:

- You must observe all existing laws, standards, policies, and regulations regarding material published on Nord Anglia's behalf, including laws governing the use of trademarks, copyrighted materials, patents, defamation and privacy laws, and laws governing the right of publicity. Understand and abide by any legal or regulatory requirements imposed on social media use. This includes all regulations promulgated by the Federal Trade Commission (FTC) and any other agency or entity with legal jurisdiction.
- You must establish accountability or ownership relating to any Nord Anglia Education information or publication posted or linked to on a publically accessible location.

- Any misspelled words or bad grammar on Nord Anglia Education’s social media channels can reflect negatively on our family of schools. Remember to double check all materials before publishing.
- You must also ensure that you do not share images or videos of children if we do not have parental consent to do so.
- You will be held accountable for the information you share in online activities. Remember that anything that is published may be public for an indefinite period of time. As such, use caution and make sure your actions reflect Nord Anglia’s positive brand attributes.

Employees should not use social networking sites such as Facebook, blogs, Twitter, etc. for classroom communication or schoolwork collaboration without permission from your principal, and all such use must be configured so as to allow full access and transparency to the principal or other employees as designated by the principal.

Nord Anglia Education and our schools use of social hubs to promote and showcase Nord Anglia initiatives such as our collaborations with The Juilliard School, Massachusetts Institute of Technology, Kings College London or UNICEF, or Global Campus and Nord Anglia University. Information and posts, if they feature specified hashtags, are drawn in from our schools around the world from trusted sources and scanned using a 3rd party aggregation tool.

Personal Use of Social Media in the Workplace

Nord Anglia is aware that employees may send personal communications through the organisation’s technology systems (including electronic and telephonic communications). This is permitted on the condition that all the procedures and rules set out in Nord Anglia policies are complied with. We expect you to limit such personal use to a minimum and strictly prohibit personal use of our technology systems which absorbs a large amount of system resources, distracts you from your duties, or that can be considered excessive by Nord Anglia Education, in its sole discretion. Be aware, however, that if you choose to make use of our facilities for personal correspondence, you can expect very little privacy because Nord Anglia may need to monitor communications.

Please note that the procedures and policies outlined in this policy, and in any related policy, may be reviewed or changed at any time. You will be alerted to important changes.

All of Nord Anglia Education’s other policies that might apply to use of social media remain in full force and effect. Social media should never be used in a way that would violate any other Nord Anglia or school policy, infringe on Nord Anglia Education’s or third party copyrights, trademarks, and other intellectual property, disclose any confidential, proprietary information, or violate any law, regulation or ethical standard related to the managing and running of our schools.

Beyond the mandatory restrictions on use and disclosure of the organisation’s confidential information and intellectual property, employees should not do anything to jeopardize such confidential information and intellectual property through use of social media. In addition, employees should avoid misappropriating or

infringing the intellectual property of other companies and individuals, which can create liability for employees and Nord Anglia Education.

No expectation of privacy

The contents of the Nord Anglia Educations' IT resources and communications systems are the property of Nord Anglia Education. Therefore, employees/volunteers should have no expectation of privacy whatsoever in any message, files, data, document, facsimile, telephone conversation, social media post, conversation or message, or any other kind of information or communications transmitted to, received or printed from, or stored or recorded on the company's electronic information and communications systems.

Employees and all adults engaged on Nord Anglia business whether paid or unpaid are expressly advised that in order to prevent misuse, Nord Anglia Education reserves the right to monitor, intercept and review, without further notice, every employee's activities using the company's IT resources and communications systems, including but not limited to social media postings and activities, and all employees are deemed to have consented to such monitoring by use of such resources and systems. This might include, without limitation, the monitoring, interception, accessing, recording, disclosing, inspecting, reviewing, retrieving and printing of transactions, messages, communications, postings, log-ins, recordings and other uses of the systems as well as keystroke capturing and other network monitoring technologies.

It is Nord Anglia Education's policy not to monitor personal communications. Electronic communications which appear to be personal or include personal content may however fall within monitored communications where there are very clear grounds for suspicion that applicable legislation or Group Policies have been violated and such communications are reasonably considered to be relevant to a resulting investigation. Where required by law, in defence of legal proceedings, pursuant to legal privilege, or as necessary to support disciplinary proceedings, data may be stored and disclosed in accordance with the appropriate HR and/or legal process.

Nord Anglia Education may also store copies of such data or communications for a period of time after they are created and may delete such copies from time to time without notice. (Subject to applicable law)

Guidelines for Employees' for responsible use of social media

General rules

- **Identify yourself:** The value of social media is diminished when people hide behind a pseudonym or an anonymous post. If you disclose your affiliation as an employee of Nord Anglia, it is recommended that you also include a disclaimer that your views do not represent the views of Nord Anglia Education. For example, consider such language as, "The views in this posting do not represent the views of my employer." Keep in mind, however, that such disclosure and disclaimer may not absolve you or Nord Anglia Education of legal liability for your online activities.
- **Be honest:** Tell the truth, and if you find you have made a mistake, issue a clarification or withdrawal and make it clear that you have done so. However, you should be aware that honesty is not always a defence to various liabilities you may incur on behalf of yourself or others as result of your online activities.
- **Take responsibility:** Nord Anglia employees are personally liable for the content they publish on social media sites. Be mindful that what you publish will be public for a long time and may have legal consequences for you and Nord Anglia. Do not post anything that is likely to bring Nord Anglia Education's reputation into disrepute.
- **Separate opinions from facts:** Make sure your audience can see the difference. However, your online activity may result in legal liability for you or Nord Anglia even if you clearly indicate that your statement is only your personal opinion.
- **Protect your privacy:** Do not disclose any personal information beyond your name, role and workplace.
- **Be respectful:** Do not post any material that is obscene, defamatory, libellous, threatening or harassing to another person or entity. This includes comments about Nord Anglia, its students and their families, employees, partners and competitors. Never post anything that is derogatory towards pupils or their families and where possible avoid posting anything that is likely to lead to a parental complaint. By the same token do not post anything that could be seen as derogatory about Nord Anglia Education employees.
- **Confidential information:** Do not reveal confidential information about Nord Anglia in a personal online posting. This might include revealing information relating to Nord Anglia students, parents, clients, business plans, policies, employees, financial information or internal discussions. Consult your line manager, Headteacher or Principal if you are unclear about what might be confidential. Do not post anything that could be seen as being personal or sensitive information about any student or their family.
- **Accepting requests:**
 - Neither supervisors nor direct reports should feel pressured to accept any requests from anyone at Nord Anglia.

- Teachers must set their personal social networking sites to 'private' so students can't access them.
 - Employees should never initiate a connection request via any social media platform with current students. If you receive a request from a current student to connect or communicate through a personal social media site, decline the request. A suggested response is: "Please do not be offended, but I cannot accept your request. It's against Nord Anglia policy to connect with current students on social media."
 - Nord Anglia Education &/or our schools may wish to cultivate connections via social media with current and former students. This will be managed through groups set up expressly for this purpose. These groups will be managed by representatives of our schools and/or the Central Marketing and Admissions team. This is a good way for us to keep in touch with students without the issues that are associated with one to one connections between individual employees and students.
- **Use good judgment and common sense:** Remember that anything you say can reflect on Nord Anglia, even if you include a disclaimer. Always remember that your statements have the potential to result in liability for yourself and Nord Anglia.
 - **Respect and comply with terms of all sites you visit:** Do not expose yourself, Nord Anglia or schools to legal risk by using a social media site in violation of its terms of use.

Safeguarding Issues

Communicating with both current and former pupils via social networking sites or via other non-school related mechanisms such as personal e-mails and text messages can lead to employees being vulnerable to serious allegations concerning the safeguarding of children and young people.

In order to make best use of the many educational and social benefits of technologies, pupils need opportunities to use and explore the digital world, using multiple devices from multiple locations. It is recognised that E-safety risks are posed more by behaviours and values than the technology itself.

Adults working in this area must therefore ensure that they establish safe and responsible online guidelines and acceptable user policies. All schools must therefore have their own acceptable user's policy. This policy/ guidance must detail the way in which all technologies may and may not be used and identify the potential sanctions for misuse. Learning Platforms are now widely established and clear agreement by all parties about acceptable and responsible use is essential.

This means that Nord Anglia Education and all our schools should:

- have in place an ICT Acceptable Use Policy (AUP);
- self-review E-Safety policies in schools regularly in the light of new and emerging technologies;
- have a communication policy which specifies acceptable and permissible modes of communication;
- ensure communication between pupils and adults, by whatever method, takes place within clear and explicit professional boundaries. This includes the wider use of technology such as mobile phones, text

messages, e-mails, digital cameras, video, web-cams, websites and blogs. Adults should not share any personal information with a child or young person. They should not request or respond to any personal information from the child/young person other than that which might be appropriate as part of their professional role. Adults should ensure that all communications are transparent and open to scrutiny.

This means that adults should:

- ensure that personal social networking sites are set at private and pupils are never listed as approved contacts;
- never use or access social networking sites of pupils;
- not give their personal contact details to pupils, including mobile telephone number;
- only use equipment e.g. mobile phones, provided by school/service to communicate with children, making sure that parents have given permission for this form of communication to be used;
- only make contact with children for professional reasons and in accordance with any school/service policy;
- recognise that text messaging should only be used as part of an agreed protocol and when other forms of communication are not possible;
- not use web-based or any other communication channels to send personal messages to a child/young person or their families without express permission of your line manager or the Principal/Headteacher;
- avoid any form of on-line, electronic (or otherwise) relationship with former pupils. This is especially important with pupils who are under 18.

Adults should be circumspect in their communications with children so as to avoid any possible misinterpretation of their motives or any behaviour which could be construed as grooming. They should not give their personal contact details to pupils including e-mail, home or mobile telephone numbers, unless the need to do so is agreed with senior management and parents/carers. Email or text communications between an adult and a child/young person outside agreed protocol may lead to disciplinary and/or criminal investigations. This also includes communications through internet based web sites.

Above all do nothing that is likely to bring into question your suitability to work for Nord Anglia Education or your suitability to work with children or young people.

Internet and e-mail systems should only be used in accordance with the Nord Anglia/school policy.

Note: in the context of this policy and safeguarding issues, the term adult is used rather than employees because in schools the policy should be applied to all adults whether employees, volunteers or contractors.

Expectations for schools:

- That this document is shared with all staff/volunteers and that it is specifically referred to when inducting new members of staff/volunteers into Nord Anglia Education and/or any of our schools.
- That appropriate links are made between this document and Nord Anglia Education's IT policy, Code of Conduct, Safeguarding guidance for Safer Working Practice and Safeguarding and Child Protection Policy.

Compliance with this Policy

Failure to comply with this policy may result in disciplinary action being taken under Nord Anglia Education's disciplinary procedures, which may include summary dismissal, and/or in the withdrawal of permission to use the firm's equipment for personal purposes. In the case of volunteers this may result in their services being terminated immediately.

If there is anything in this policy that you do not understand, please discuss it with your line manager/Headteacher/Principal.

If you are uncertain about whether information or content you intend to post or upload is a violation of a Nord Anglia policy, rule, expectation or standard of conduct, the employee should seek guidance from their line manager, Headteacher/Principal, human resources, or the Chief Legal Officer.

Frequently asked Questions (FAQ's)

Q1. Should I use my mobile phone to take photographs or video of students?

School trips are a common situation where photography by pupils and staff should be encouraged, but there are potential dangers.

The safest approach is to avoid the use of personal equipment and to use a school-provided item. One potential danger is an allegation that an adult has taken an inappropriate photograph. With a personal camera it would be more difficult for the adult to prove that this was not the case. With school equipment there is at least a demonstration that the photography was consistent with school policy. Care should also be taken that photographs are stored appropriately. For instance, to copy the photographs onto a personal laptop as opposed to a school allocated laptop might make it difficult to retain control of how the picture is used. Memory cards, memory sticks and CDs should only provide a temporary storage medium. Once photographs are uploaded to the appropriate area of the school network, images should be erased immediately from their initial storage location.

It is important to continue to celebrate achievements of pupils through the appropriate use of photography in communicating with parents and the community. It is, however, essential to do this safely. You should also confirm whether any students (or their parents) have not consented to their picture being taken or being recorded on film via their PICS form which is collected on enrolment and at the start of each academic year.

Q2. Should I continue to use my Social Networking site?

Social networking is a way of life for most young people and many adults. However, adults working with children and young people especially should review their use of social networks. Strong passwords should be used and security settings should be applied so that you control all access to your profile.

Information once published, e.g. photographs, blog posts etc. is impossible to control and may be manipulated without your consent, used in different contexts or further distributed. Some adults have been caught out by posting amusing remarks about the school or colleagues, only to find them republished elsewhere by their 'friends'. Even innocent remarks such as an interest in "Gang Wars" could be misinterpreted (this is actually a game).

False social networking sites have been set up by pupils and staff with malicious information about staff.

Currently only a few public social networking sites authorise their members and use automated registration systems, which provide limited checks.

Social networking is an excellent way to share news with family and friends. Providing the security levels have been set correctly and a strong password used, information should remain private. The danger is that few people understand profile privacy settings. The minimum age of use of a social networking website must be observed by a school, even though many pupils disregard this legal requirement.

Some instant messaging applications such as MSN have a facility to keep log of conversations, which could be used to protect staff in case an allegation is made. "Don't publish anything that you would not want your mum, children or line manager to see, either now or in ten years' time!"

Q3. Should I have pupils as friends on instant messaging services?

Communication between adults and children, by whatever method, should take place within clear and explicit professional boundaries. Adults should not share any personal information with the child or young person. They should not request, or respond to, any personal information from the child/young person other than that which might be appropriate as part of their professional role. Adults should ensure that all communications are transparent and open to scrutiny.

Online communication provides excellent opportunities for collaborative work between groups of pupils. Monitoring or tuition, where appropriately arranged, could guide and enhance such activities.

Consideration should be given as to how this type of communication might appear to a third party. Compared with a conversation in school the use of new technology inevitably increases the potential for messages to be seen out of context or misinterpreted.

If instant messaging and other social networking sites are to be used with pupils, a separate and approved school/Organisation account should be set up for this purpose, with the agreement of senior management/Principal.

Staff need an online environment which is under their control. The first requirement is that you know who you are talking to; users must be authenticated. Schools in particular should have a range of security features available to them.

Q4. What is my responsibility for the use of my Nord Anglia/school laptop at home?

Things that can go wrong include:

- Access to wider sites by family members, for instance a gaming site or internet shopping would increase the possibility of virus attack and identity theft.
- If another member of the family or a friend is allowed to use the computer it is difficult to ensure that the use has been appropriate, for instance that confidential information has not been accessed. Adults vary enormously in their judgements as to what is appropriate.

Some adults may feel that access via a school/Nord Anglia laptop to adult material outside school hours and at home is appropriate. It is not. There is always a possibility that this material might be accidentally seen by a child/young person but these sites often carry hidden virus's and enable unwanted 'pop-ups' to appear on screen.

Adults need to remember that in order for anyone else to use a Nord Anglia/school laptop in the home setting, they would need to be logged on by the person responsible for the laptop. With this in mind, think about who would be culpable in certain situations if something was to go wrong.

Personal use of technology by adults has been shown to increase competence and confidence and should therefore be encouraged. Staff should refer to the school for the expectation on the personal use of school laptops. Increasingly the use of a school computer for non-professional use is being explicitly banned.

There are no circumstances that justify adults possessing indecent images of children. Adults who access and possess links to such websites will be viewed as a significant and potential threat to the children. Adults should therefore ensure that they must have absolute control of a Nord Anglia/school laptop or any other electronic device, allocated for their use.

Q5. What is inappropriate material?

Inappropriate is a term that can mean different things to different people. It is important to differentiate between 'inappropriate' and 'unlawful' and 'inappropriate' but 'lawful'. All staff should be aware that in the former case investigation may lead to criminal investigation, prosecution, dismissal (and in the case of teachers being barred from the profession). In the latter it can still lead to disciplinary action, dismissal and barring even if there is no criminal prosecution.

Unlawful/Illegal

Possessing or distributing indecent images of a person under 18 and/or viewing such images on-line may well constitute possession even if the material is not saved. What is regarded as indecent would ultimately be down to Nord Anglia Education, a police officer or jury to decide.

In the UK, USA and in many European countries the police have a grading system for different types of indecent images.

Remember that children will have been coerced or forced into posing for such images and are therefore victims of child sexual abuse.

Note: Hate/Harm/Harassment

General: There is a range of offences in the UK, USA and much of Europe to do with inciting hatred on the basis of race, religion, sexual orientation etc.

Individual: There are particular offences to do with harassing or threatening individuals – this includes cyberbullying by mobile phone, social networking sites etc. It is an offence to send indecent, offensive or threatening messages with the purpose of causing the recipient distress or anxiety.

Inappropriate but not necessarily unlawful/illegal.

Think about this in respect of professionalism and being a role model. The scope here is enormous, but bear in mind that “actions outside of the workplace that could be as serious as to fundamentally breach the trust and confidence placed on the employee” may constitute gross misconduct.

Examples taken from real events:

- Posting offensive or insulting comments about the school on Facebook
- Accessing adult pornography on school computers during break
- Making derogatory comments about pupils or colleagues on social networking sites
- Contacting pupils by e-mail or social networking without senior approval
- Trading in sexual aids, fetish equipment or adult pornography

Q6. How should I store personal data safely?

Teachers in schools and other staff often find it convenient to write pupil reports or staff appraisals and references at home. This may require access to confidential personal information. All personal information must however be kept secure. The storage of data on a hard disk or other means is basically insecure. Making such storage secure may include password protection, encryption of data and locking the computer when not in use. Physical risks including mislaying a memory stick and laptop theft from a vehicle are all too common. Consider approaches such as not storing information unless necessary and deleting files after use. The safest long-term storage location may be the Nord Anglia/school network, which should have a remote backup facility and suitable web filtering. You must take all reasonable steps to ensure that any personal information that you are processing is stored securely.

All staff are strongly advised to ensure that they understand the Nord Anglia/school policy regarding data protection. National and international policy is developing rapidly in this area. To lose control of personal data while not complying with the school policy would be difficult to defend in any subsequent litigation.

Q7. How can I use ICT appropriately to communicate with young people?

Young people should be encouraged to report any concerns, which may involve the use of technology, e.g. a pupil might prefer to text a report about bullying, rather than arrange a face to face discussion.

Friendly verbal banter between adult and pupil may not be inappropriate, but it might look very different if carried out via e-mail or messenger and might lead to difficulties if misinterpreted, forwarded or used out of context. Care in the use of automatic signatures or email addresses is required e.g. “Sexylegs” is not an appropriate signature for either pupil or adult when in an educational setting.

Adults should be circumspect in their communications with children and young people so as to avoid any possible misinterpretation of their motives or any behaviour which could be construed as grooming.

Q8. As a teacher, how can I safely monitor school network use?

Filtering or recording network usage will only be effective as a safeguard if monitored carefully to both notice and report inappropriate access or usage. Often this places a new responsibility on technical staff that they may not be trained for. This responsibility can become onerous in a school situation if a pupil or staff member is apparently implicated in inappropriate or illegal activity.

It is wrong to assume that filtering and monitoring are simply technical ICT activities solely managed by the network staff. Some technical staff have indeed taken on this wider responsibility to help ensure that ICT use is appropriate and beneficial. However technical staff should not be expected to make judgements as to what is inappropriate material or behaviour without support and supervision from the Senior Leadership team/Line manager. The Senior Leadership Team/line manager will require assistance from technical staff as well.

In a school situation any concerns raised should also involve the school Designated Safeguarding Lead to assist in any decision making.

A technician might, with the best of intent, check sites that a user has visited and email images to alert a colleague. Should the images prove to be illegal the technician may have committed a criminal offence. A defence may be that the technician was acting within a published Nord Anglia/school procedure but staff should ensure that they receive a specific, written request to perform this work.

Should an incident of concern occur there should be a clear route for immediate reporting to a senior leader/line manager. Procedures to preserve evidence by unplugging/locking a computer or locking an account need to be in place.

Q9. Can my school limit private on-line publishing?

As a teacher I have been asked to sign a “Professional Conduct Agreement” that requires me to be careful when using ICT out of school. Surely that is my own business?

One situation included a teacher complaining about a parent’s rudeness. Had the conversation remained private as no doubt intended, this might be regarded as simply letting off steam. However, because a social networking site was used with incorrect privacy settings, an unintended audience was included and a complaint made.

The situation is not new. Teachers discussing a pupil in a shop queue might be overheard by a parent. However, the technology enables messages to be recorded, edited maliciously, used out of context, re-published or used as evidence.

The mode of use of social networking and instant messaging is often conversational with a rapid interchange of remarks. It is easy to stray from a non-school conversation between friends to professional matters and perhaps not realise the lack of control over audience.

Teachers using technology should either be fully conversant with the security arrangements for the site in use or better avoid any information that could compromise their professional integrity.

Q10. How do I ensure safer online activity in the primary classroom?

Most internet use in schools is safe, purposeful and beneficial to pupils and staff. However, there is always an element of risk, even an innocent search can occasionally turn up links to adult content or imagery.

Planning and preparation is vital and the safest approach when using online material in the classroom is to test sites on the school system before use. For very young pupils you should direct them to a specific website or a selection of pre-approved websites and avoid using search engines.

When working with older pupils, select appropriate and safe search engines. Appropriate search terms should be used and pre-checked. Consider carefully the age, ability and maturity of all pupils when planning online activities. When encouraging pupils to publish work online, schools should consider using specific safe sites and learning environments.

If inappropriate material is discovered then turn off the monitor, reassure the pupils and to protect yourself you need to log and report to a member of the senior leadership team/line manager. Avoid printing or capturing any inappropriate material.

Linked Documents

Nord Anglia Education Code of Conduct and Ethics
 Relevant School/Office Employee Handbook
 External Communications Policy
 Media Relations Policy
 Policy Statement – Guidelines for Corporate Disclosure (Regulation FD Policy)
 Information Technology Acceptable Users Policy
 Privacy Policy
 Internal Communications Policy
 General use of IT policy
 Nord Anglia Education Safeguarding and Child Protection Policy
 Nord Anglia Education Guidance for Safer Working Practice
 Nord Anglia Education Disciplinary Policy

Modification History

Policy Number: MAC-4.1

Policy Name: Social Media

Description: Communications and enquiries protocols

Version No.	Amendments	Issue Date	Issued By
v1	First Release	12 July 2016	Richard Seymour, Head of Digital
v2	Comments/edits	14 July 2016	Group Finance
V3	Draft release	16 March 2017	Barry Armstrong, Head of Safeguarding
V4	Updated release	01 April 2017	Sarah Doyle, Head of Digital