



Electronic Information and Communication Policy (including Social Media)

Introduction

The Centre's electronic information and communication systems and equipment are intended to promote effective communication and working practices throughout the business and are critical to the success of our provision of excellent service.

However, it also brings with it certain risks, some of which may involve potential legal and financial liabilities for both us and you, e.g.:

- inadvertently entering into contracts or commitments on behalf of us;
 - introducing viruses into our systems;
 - breaching copyright or licensing rights;
 - breaching data protection rights;
 - breaching confidentiality and security;
 - defamation; and/or
- bullying, harassment and discriminatory conduct.

This policy aims to guard against those risks. It is therefore important that all staff read the policy carefully and ensure that they use the internet, email and other communication systems in accordance with it. If you are unsure whether something you are about to do complies with this policy, you should seek advice from your line manager.

At Norcot Early Years Centre we recognise that social media describes a range of online applications that enable and encourage interactive communication between users. Used well, social media can be part of collaborative working and sharing information.

This policy applies to all Centre staff regardless of their employment status. This policy does not form part of the terms and conditions of employee's employment with the Centre and is not intended to have contractual effect. It does however set out the Centre's current practices and required standards of conduct and all staff are required to comply with its contents. **Breach of the provisions of this policy will be treated as a disciplinary offence which may result in disciplinary action up to and including summary dismissal in accordance with the Centre's Disciplinary Policy and Procedure.**

This Policy may be amended from time to time and staff will be notified of any changes no later than one month from the date those changes are intended to take effect.

All staff should consider how their reputation and that of the Centre might be affected by how they communicate and conduct themselves online.

The use by staff and monitoring by the Centre of its electronic communications systems is likely to involve the processing of personal data. Therefore, it is regulated by the UK General Data Protection Regulation (UK GDPR) and all data protection laws and guidance in force.

Staff are referred to the Centre's Data Protection Policy for further information. The Centre is also required to comply with the Regulation of Investigatory Powers Act 2000, the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 and the principles of the European Convention on Human Rights incorporated into U.K. law by the Human Rights Act 1998.

All members of staff are required to comply with the provisions set out in this policy at all times to protect The Centre's electronic systems from unauthorised access or harm. Breach of this policy will be regarded as a disciplinary offence and dealt with under the Centre's disciplinary procedure and in serious cases, may be treated as gross misconduct leading to summary dismissal.

The Centre has the right to monitor all aspects of its systems, including data which is stored under the Centre's computer systems in compliance with the UK GDPR

Scope and Purpose of this Policy

The Centre recognises that electronic information and the internet provides unique opportunities to participate in interactive discussions and share information on particular topics using a wide variety of social media, such as email, Facebook, Twitter, LinkedIn, blogs and Wikipedia. However, staff use of these systems can pose risks to the Centre's confidential and proprietary information, its reputation and it can jeopardise our compliance with our legal obligations.

To minimise these risks, avoid loss of productivity and to ensure that our IT resources and communications systems are used only for appropriate work-related purposes, all Centre staff are required to comply with the provisions in this policy.

It applies to the use of social media for both work and personal purposes, whether during work hours or otherwise. The policy applies regardless of whether the social media is accessed using our IT facilities and equipment or equipment belonging to members of staff.

Disciplinary action may be taken regardless of whether the breach is committed during working hours and regardless of whether the Centre's equipment or facilities are used for the purpose of committing the breach. Any member of staff suspected of committing a breach of this policy will be required to co-operate with our investigation, which may involve handing over relevant passwords and login details. Staff may be required to remove internet postings which are deemed to constitute a breach of this policy. Failure to comply with such a request may in itself result in disciplinary action.

Prohibited use and breach of this policy

We consider this policy to be extremely important. Any breach of the policy will be dealt with under our disciplinary policy. In certain circumstances, breach of this policy may be considered gross misconduct and may result in

immediate termination of employment or engagement without notice or payment in lieu of notice. In addition, or as an alternative, we may withdraw an individual's internet and/or email access.

Examples of matters that will usually be treated as gross misconduct include (this list is not exhaustive):

- unauthorised use of the internet;
- creating, transmitting or otherwise publishing any false and defamatory statement about any person or organisation;
- creating, viewing, accessing, transmitting or downloading any material which is discriminatory or may cause embarrassment to other individuals, including material which breaches the principles set out in our equality, diversity and inclusion policies;
- accessing, transmitting or downloading any confidential information about The Centre and/or any of our staff and/or current, former or prospective pupils or parents, suppliers, contractors or other such third parties, except where authorised in the proper performance of your duties;
- accessing, transmitting or downloading unauthorised software; and
- viewing, accessing, transmitting or downloading any material in breach of copyright.

Who is covered by this policy?

This policy covers all individuals working at all levels and grades within the Centre, including senior managers, officers, governors, employees, consultants, contractors, trainees, homeworkers, part-time and fixed-term employees, casual and agency staff and volunteers (collectively referred to as **Staff** in this policy).

Third parties who have access to our electronic communication systems and equipment are also required to comply with this policy.

Personnel responsible for implementing the policy

The Board of Governors have overall responsibility for the effective operation of this policy, but have delegated day-to-day responsibility for its operation to the Headteacher.

Responsibility for monitoring and reviewing the operation of this policy and making recommendations for change to minimise risks also lies with the Headteacher and SMT.

All line Managers have a specific responsibility for operating within the boundaries of this policy, ensuring that all staff understand the standards of behaviour expected of them and taking action when behaviour falls below its requirements.

All Centre Staff are responsible for the success of this policy and should ensure that they take the time to read and understand it. Any misuse of social media should be reported to the Headteacher in the first instance.

Compliance with related policies and agreements

Social media should never be used in a way that breaches any of our other policies. If an internet post would breach any of our policies in another forum, it will also breach them in an online forum. For example, employees are prohibited from using social media to:

- Breach our Electronic information and communications systems policy;
- Breach our obligations with respect to the rules of relevant regulatory bodies;
- Breach any obligations they may have relating to confidentiality;
- Breach our Disciplinary Rules;
- defame or disparage the Centre, its Staff, its pupils or parents, its affiliates, partners, suppliers, vendors or other stakeholders;

- Harass or bully other Staff in any way or breach our Anti-harassment and bullying policy;
- Unlawfully discriminate against other Staff or third parties or breach our Equal opportunities policy;
- Breach our Data protection policy (for example, never disclose personal information about a colleague or pupils online);
- Breach any other laws or ethical standards (for example, never use social media in a false or misleading way, such as by claiming to be someone other than yourself or by making misleading statements).
- Staff should never provide references for other individuals on social or professional networking sites, as such references, positive and negative, can be attributed to the Centre and create legal liability for both the author of the reference and the organisation.

Personal use of social media

Personal use of social media is never permitted during working time or by means of our computers, networks and other IT resources and communications systems. Examples of social media include Facebook, WhatsApp, LinkedIn, Twitter, Tik Tok, Instagram, Snap Chat (this list is not exhaustive).

Staff should not use a work email address to sign up to any social media and any personal social media page should not make reference to their employment with the Centre (excluding LinkedIn, where prior permission is sought from Business Manager).

Staff must not take photos or posts from social media that belongs to the Centre for their own personal use. Staff may share specific posts from the Centre Facebook page with prior permission e.g., fundraiser events.

Staff must not share Centre communication that is for staff only, with parents of the Centre, friends or others e.g., staff meeting minutes, SMT minutes, (this list is not exhaustive).

Monitoring

The contents of our IT resources and communications systems are the Centre's property. Therefore, staff should have no expectation of privacy 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 our electronic information and communications systems.

The Centre reserves the right to monitor, intercept and review, without further notice, staff activities using our IT resources and communications systems, including but not limited to social media postings and activities, to ensure that our rules are being complied with and for legitimate business purposes and you consent to such monitoring by your acknowledgement of this policy and your 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.

The Centre may 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.

All Staff are advised not to use our IT resources and communications systems for any matter that he or she wishes to be kept private or confidential from the Centre.

Educational or Extra Curricular Use of Social Media

If your duties require you to speak on behalf of the Centre in a social media environment, you must follow the protocol outlined below.

The Headteacher may require you to undergo training before you use social media on behalf of the Centre and impose certain requirements and restrictions with regard to your activities.

Likewise, if you are contacted for comments about the Centre for publication anywhere, including in any social media outlet, you must direct the inquiry to the Headteacher and must not respond without advanced written approval.

Photographs for use of Social Media

Any photos for social media posts may only be taken using Centre cameras/devices or devices that have been approved in advance by parental permission forms. Where any device is used that does not belong to the Centre all photos must be deleted immediately from the device, once the photos have been uploaded to a device belonging to the Centre.

Staff Protocol for use of Social Media

- Where any post is going to be made on the Centre's own social media the following steps must be taken:
- Ensure that permission from the child's parent has been sought before information is used on social media (via consent form for use of photos)
- Ensure that there is no identifying information relating to a child(ren) in the post - for example any certificates in photos are blank/without names or the child's name cannot be seen on the piece of work.
- The post must be a positive and relevant post relating to the children, the good work of staff, the Centre or any achievements.
- Social Media can also be used to issue updates or reminders to parents/guardians and Business Manager will have overall responsibility for this.
- The proposed post must be presented to Admin Team for confirmation that the post can 'go live' before it is posted on any social media site.
- The Admin Team will post the information, but all staff have responsibility to ensure that the Social Media Policy has been adhered to.
- As part of KCSIE 2023 changes and part of due diligence checks, online searches and checks for new members of staff are recommended. A question must be asked at interview to ask if they would like to tell us anything regarding their social Media platforms ahead of the checks.

Protecting our Business Reputation

Staff must not post disparaging or defamatory statements about:

- The Centre;
- Current, past or prospective Staff as defined in this policy
- Current, past or prospective pupils
- Parents, carers or families of (iii)
- The Centre's suppliers and services providers; and
- Other affiliates and stakeholders.

Staff should also avoid social media communications that might be misconstrued in a way that could damage the Centre's reputation, even indirectly.

If Staff are using social media, they should make it clear in any social media postings that they are speaking on their own behalf. Staff should write in the first person and use a personal rather than Centre e-mail address when communicating via social media.

Staff are personally responsible for what they communicate in social media. Staff should remember that what they publish might be available to be read by the masses (including the Centre itself, future employers and social acquaintances) for a long time. Staff should keep this in mind before they post content.

If Staff disclose whether directly or indirectly their affiliation to the Centre as a member of Staff whether past, current or prospective, they must also state that their views do not represent those of the Centre.

Staff must ensure that their profile and any content posted are consistent with the professional image they are required to present to colleagues, pupils and parents.

Staff must avoid posting comments about confidential or sensitive Centre related topics. Even if Staff make it clear that their views on such topics do not represent those of the Centre, such comments could still damage the Centre's reputation and incur potential liability.

If a member of Staff is uncertain or concerned about the appropriateness of any statement or posting, he or she should refrain from making the communication until he or she has discussed it with his Line Manager or SMT.

If a member of Staff sees content in social media that disparages or reflects poorly on the Centre, it's Staff, pupils, parents, service providers or stakeholders, he or she is required to report this in the first instance to the Headteacher without unreasonable delay. All staff are responsible for protecting the Centre's reputation.

Respecting intellectual property and confidential information

Staff should not do anything to jeopardise Centre confidential information and intellectual property through the use of social media.

In addition, Staff should avoid misappropriating or infringing the intellectual property of other Centre's, organisations, companies and individuals, which can create liability for the Centre, as well as the individual author.

Staff must not use the Centre's logos, brand names, slogans or other trademarks, or post any of our confidential or proprietary information without express prior written permission from the Headteacher.

To protect yourself and the Centre against liability for copyright infringement, where appropriate, reference sources of particular information you post or upload and cite them accurately. If you have any questions about whether a particular post or upload might violate anyone's copyright or trademark, ask the Headteacher in the first instance before making the communication.

Respecting colleagues, pupils, parents, clients, service providers and stakeholders

Staff must not post anything that their colleagues, the Centre's past, current or prospective pupils, parents, service providers or stakeholders may find offensive, including discriminatory comments, insults or obscenity.

Staff must not post anything related to colleagues, the Centre's past, current or prospective pupils, parents, service providers or stakeholders without their advanced written permission.

E-mail etiquette and content

The Centre's e-mail is intended to promote effective professional communication between staff, parents and external business. Access to e-mail is provided for work purposes only.

Staff should always consider if e-mail is the appropriate medium for a particular communication. The Centre encourages all members of staff to make direct contact with individuals rather than communicate by e-mail wherever possible to maintain and enhance good working relationships.

Messages sent on the e-mail system should be written as professionally as a letter and should be concise and directed only to relevant individuals on a need-to-know basis. The content and language used in the message must be consistent with the Centre's best practice.

E-mails should never be sent in the heat of the moment or without first checking the content and language and considering how the message is likely to be received.

All members of staff should remember that e-mails can be the subject of legal action for example in claims for breach of contract, confidentiality, defamation, discrimination, harassment etc. against both the member of staff who sent them and the Centre. Staff should take care with the content of e-mail messages, as incorrect or improper statements can give rise to personal liability of staff and to liability of the Centre in the same way as the contents of letters.

Staff should assume that e-mail messages may be read by others and not include in them anything which would offend or embarrass any reader, or themselves, if it found its way into the public domain. The Centre standard disclaimer should always be used on every e-mail.

SMT and office staff should ensure that they access their emails regularly and delete junk mail, and actioned emails in accordance with the UK GDPR data retention policy. Staff should endeavour to respond to emails marked 'high

priority' as soon as is reasonably practicable. A work email address is provided for all staff as it is considered an effective and secure means of communication.

Members of staff are strictly forbidden from sending abusive, obscene, discriminatory, racist, harassing, derogatory or defamatory messages. If such messages are received, they should not be forwarded and should be reported to SMT immediately.

If you feel that you have been harassed or bullied, or are offended by material sent to you by a colleague via e-mail, you should inform the Headteacher.

As general guidance, staff must not:

- Send any e-mail, including resending and forwarding, containing sexually explicit or otherwise offensive material either internally or externally;
- Send any e-mail communication which may be regarded as harassing or insulting. Complaints about the performance or service of other departments or individuals must be made on a face-to-face basis in accordance with normal and courteous practice;
- Send or forward chain mail, junk mail, cartoons, jokes or gossip either within or outside the Centre;
- Sell or advertise using the systems or broadcast messages about lost property, sponsorship or charitable appeals
- Contribute to system congestion by sending trivial messages or unnecessarily copying or forwarding e-mails to those who do not have a real need to receive them;
- Agree to terms, enter into contractual commitments or make representations by e-mail unless the appropriate authority has been obtained. A name typed at the end of an e-mail is a signature in the same way as a name written in ink at the end of a letter;
- Send messages from another worker's computer or under an assumed name unless specifically authorised;
- Send confidential messages via e-mail or the internet, or by other means of external communication which are known not to be secure;
- e-mail may normally only be used to communicate internally with colleagues and students (where appropriate and necessary) and externally to parents, suppliers and third parties on academic/service-related issues. Urgent or important messages to family and friends are permitted but must be of a serious nature;

The Centre recognises that it is not always possible to control incoming mail. Any material which would be considered as inappropriate or unprofessional, sexually explicit or offensive should be deleted at once and not forward it to any internal or external recipient, other than internally to the data protection officer in order to report a breach of this or another policy. If you believe you may have been bullied, harassed, sexually harassed or victimised, we encourage you to report this. Any member of staff who finds that they are receiving such communications from known sources is responsible for contacting that source in order to request that such communication is not repeated.

Staff who receive an e-mail which has been wrongly delivered should return it to the sender of the message and delete the email as soon as possible to minimise any further risk to individuals whose data could be breached. If the e-mail contains confidential information or inappropriate material (as described above) it should not be disclosed or forwarded to another member of staff or used in any way

Our ICT Support should be informed as soon as reasonably practicable.

Emails—monitoring

We may monitor the email and instant messaging systems or network in the workplace for the following reasons:

1. to determine whether they are communications relevant to the carrying on of our relevant activities;
2. if the individual is absent from work, to check communications for business calls to ensure the smooth running of the Centre;
3. to record transactions;
4. where we suspect that the individual is sending or receiving messages that are:
 - a. detrimental to us;
 - b. in breach of the individual's contract, or this policy;
 - c. in breach of data protection rights;
 - d. to monitor staff conduct;
 - e. to investigate complaints, grievances or criminal offences.

When monitoring incoming or outgoing emails, we will, unless exceptional circumstances apply:

1. look at the sender or recipient of the email and the subject heading only; and
2. avoid opening emails marked 'Private' or 'Personal'.

Use of the web and the internet

Our access to the internet is controlled by a firewall to limit inappropriate content.

Staff should not under any circumstances use Centre systems to participate in any internet chat room, post messages on any internet message board or set up or log text or information even in their own time.

Remember also that text, music and other content on the internet are copyright works. Staff should not download or e-mail such content to others unless certain that the owner of such works allows this.

The Centre's website may be found at www.norcotearlyyearscentre.co.uk. This website is intended to convey our core values and excellence in the educational sector. All members of staff are encouraged to give feedback concerning the site and new ideas and inclusions are welcome. All such input should be submitted to SMT in the first instance. Only expressly authorised and designated members of staff are permitted to make changes to the website.

Personal use of the Centre's systems

The Centre permits the incidental use of its internet, e-mail and telephone systems to send personal e-mail, browse the web and make personal telephone calls subject to certain conditions set out below.

Our policy on personal use is a privilege and not a right. The policy is dependent upon it not being abused or overused and we reserve the right to withdraw our permission or amend the scope of this policy at any time.

The following conditions must be met for personal usage to continue:

- Use must be minimal and take place substantially out of normal working hours (that is, during the member of staff's usual break time or shortly, before or after normal working hours);
- Use must not interfere with business or office commitments;

Staff should be aware that any personal use of the systems may also be monitored (see below) and, where breaches of this policy are found, action may be taken under our Disciplinary Policy and Procedure. Any excessive or

inappropriate personal use of the Centre's email facility will be treated as a disciplinary offence resulting in disciplinary action up to and including summary dismissal depending on the seriousness of the offence.

Where evidence of misuse is found the Centre may undertake a more detailed investigation in accordance with our Disciplinary Policy and Procedure, involving the examination and disclosure of monitoring records to those nominated to undertake the investigation and any witnesses or members of management involved in the disciplinary procedure.

If necessary, such information may be handed to the police in connection with a criminal investigation.

The Centre has a responsibility to ensure that it is compliant with the 7 principles of data Processing whilst monitoring staff usage of our systems.

Personal data must be:

1. Processed lawfully, fairly and in a transparent manner
2. Collected for specified, explicit and legitimate purposes
3. Adequate, relevant and limited to what is necessary in relation to the purposes for which the data is processed
4. Accurate and kept up to date
5. Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data is processed
6. Processed in a way that ensures appropriate security of personal data

The 7th principle is that:

7. Your school is responsible for complying with these principles, and must be able to show that it is complying.

Monitoring and review of this policy

SMT shall be responsible for reviewing this policy from time to time to ensure that it meets legal requirements and reflects best practice. The Board of Governors has responsibility for approving any amendments prior to implementation.

Associated Policies

Safeguarding

- Information Security Policy
- Whistle Blowing
- Code of Conduct
- Disciplinary
- Harassment
- Mobile phone, Video or Photographic Image Use Policy

Policy Agreed: October 2025

Policy to be Reviewed: Every 2 years, October 2027