E-Safety Policy (for Staff)
(including Social Media and Email)

Document Review:	**SLT**
Responsibility for Policy:	**Resources Committee**
Approved:	**19/11/2020**
Review due:	**Autumn Term 2022**

For the purpose of this policy Guildford Nursery School and Family Centre will be referred to as GNSFC.

Aim of Policy

This policy is designed to make sure that all GNSFC staff are aware of their professional responsibilities and engage in safe working practices. This policy also applies to those who, whilst not directly employed by GNSFC, may use Information Technology (I.T.) and Social Media in an official capacity on behalf of GNSFC for example, governors, volunteers or associated individuals and organisations.

Internet

The internet contains a vast array of information however not all information on the internet is accurate, complete or reliable and its validity should always critically evaluated before use.

Users shall not deliberately visit any inappropriate sites including but not limited to sites that;

- Contain pornographic content
- Promote discrimination of any kind
- Promote racial or religious hatred
- Promote illegal acts
- Contain any other information which may be offensive to staff and other parties
- Include on-line betting and gambling
- Are social networking sites other than for management of GNSFC's account
- Are chat sites
- Are dating agencies

Website

GNSFC website can be found at www.guildfordnscc.surrey.sch.uk

Websites can provide information on who has visited them. Users of the internet leave a "calling card" which enables GNSFC to work out who has visited. If the website is an inappropriate one, GNSFC's reputation could be at serious risk for which the user will be held to account.

- Material published to the website is subject to review and approval by a Line Manager or member of SLT

- Each item of information should have its provider and date of publication identified
- Permission must be obtained from the 'owner' before using images, text or other material not produced by GNSFC and authorised by SLT
- GNSFC owns the copyright to all of its own material

Photographs and Filming

GNSFC will only use images, photographs or films/videos of children or staff, with signed permission from parents or carers (in the case of children) or the individual in respect of staff. A permission form will be held on each individual pupil or staff record. Permission/consent can be withdrawn at any time either in writing or by email.

- Consent and permission forms are to be filed appropriately and kept securely in a locked cupboard.
- A spreadsheet of consent and permission will be maintained by the Admissions Manager or delegated team member.
- A spreadsheet of staff permissions will be maintained by the HR Manager (or a delegated team member).
- GNSFC may use images for the following purposes:
    - Recording keeping and assessment (children's learning journeys)
    - Displays in GNSFC
    - Brochures, leaflets, cards, posters, for internal and external marketing
    - Training and presentation purposes within GNSFC
    - Articles and events on the GNSFC website
    - Social media sites used by GNSFC

Emails

Emails are frequently used in preference to telephone conversations as a means of communicating. Whilst emails are less formal, they are more open to misinterpretation than formal letters. Emails should always adhere to the good practice guidelines as set out below. Be aware that email is not always a secure medium to send confidential information and information security needs to be considered when sending emails.

- Any emails containing personal or confidential information must only be sent by a secure, encrypted email system such as Egress. Speak to the Business Manager if you require an Egress subscription.
- No personal information, such as a pupil's name, should ever be included in the subject line of an email.
- Only authorised persons are to be the recipients of emails containing sensitive information.
- Email is disclosable under the GDPR, Freedom of Information and Data Protection legislation. Be aware that what you write in an email may be made public.
- Be aware that emails can remain in a system. Whilst you may have deleted an email, the recipient may not have done so.
- Be aware that email can form a contractual obligation. Members of staff should not enter into agreements either with other members of staff internally or with external contractors unless authorised to do so by a member of SLT.
- All email attachments should be saved into an appropriate electronic filing system or printed out and placed in secure paper files in accordance with the GNSFC Records Management Policy.
- GNSFC has a right to monitor the use of staff work email addresses.

Sending Emails

- Emails from work email accounts must be for professional purposes only
- Do not send anything in an email that could not be sent on GNSFC letter headed paper
- Do not forward chain letters, junk or spam email
- Do not forward inappropriate material, externally or internally. If you are aware of any inappropriate material report to the Headteacher or Business Manager immediately.
- Do not access emails addressed to others unless authorised to do so. This could constitute a criminal offence.
- Limit recipients to the people who really need to receive the email. Avoid the use of global or group address lists unless it is absolutely necessary. Never send on chain emails.
- When sending emails containing personal or sensitive data always respond to an authorised, approved address. All emails that are used for official business must be sent from an official business domain address.
- Having a clearly defined subject line helps the recipient to sort the email on receipt.
- A clear subject line also assists in filing all emails relating to individual projects in one place. For example, the subject line might be the name of the policy, or the file reference number.
- Ensure that the email is clearly written

    - Do not use text language or informal language in GNSFC e-mails.
    - Always sign off with a name (and contact details).
    - Make sure that you use plain English and ensure that you have made it clear how you need the recipient to respond.
    - Never write a whole email in capital letters. This can be interpreted as shouting.
    - Always spell check an email before you send it. Do not use the urgent flag unless it is absolutely necessary.
    - If possible, try to stick to one subject for the content of each email, as it will be easier to categorise it later if you need to keep the email.

- Sending large attachments (e.g. graphics or presentations) to a sizeable circulation list can cause resource problems on your network. Where possible put the attachment in an appropriate area on a shared drive and send the link round to the members of staff who need to access it.
- All emails sent should contain a signature containing the senders contact information so that the recipient(s) are aware of who the sender is. This would normally contain; name, job title, work address and telephone number.
- Ensure the GNSFC disclaimer (available from the Business Manager or HR Manager) is included below your signature/name. This mitigates risk, such as sending information to the wrong recipient, or helps to clarify GNSFC's position in relation to the information being emailed. It must also cover the fact that information is confidential, to be solely used by the intended recipient, and that the views or opinions of the sender are not necessarily those of GNSFC.

Managing Received Emails

- If you receive any inappropriate e-mail material the following actions must be taken:

    - If the sender is known to you or is not an obvious source of spam, then reply to the sender saying that you do not wish to receive such material in the future
    - If the email is unwanted but from a trusted sender open email and follow their instructions to unsubscribe from mails
    - If the sender is not known to you and is an obvious source of spam, do not read the email, right click on the message, select junk and block the sender

- Manage interruptions by turning off alerts notifying of emails received and plan times to check emails into your day.

- Use Rules and Alerts
    - By using rules and alerts members of staff can manage their inbox into theme-based folders. For example:
        - Emails relating to a specific subject or project can be diverted to a named project folder
        - Emails from individuals can be diverted to a specific folder
        - Warn senders that you will assume that if you are copied in to an e-mail, the message is for information only and requires no response from you.
    - Internally, use a list of defined words to indicate in the subject line what is expected of recipients (for example: “For Action:” FYI:” etc.)
    - Use electronic calendars to invite people to meetings rather than sending emails asking them to attend

- Use an ‘Out of Office’ message when you’re away for more than a day
- If you check your email at stated periods during the day you can use an automated response to incoming e-mail which tells the recipient when they might expect a reply.

Saving Emails
Attachments only
Where the main purpose of the email is to transfer documents, then the documents should be saved into the appropriate place in an electronic filing system or printed out and added to a paper file. The email can then be deleted.

Email text and attachments
Where the text of the email adds to the context or value of the attached documents it may be necessary to keep the whole email. The best way to do this and retain information which makes up the audit trail, is to:

- save the email in .msg format by copying and pasting into a document and saving the document in an appropriate folder
- or by clicking and dragging the email into the appropriate folder
- or by using the “save as” function to save the email in an electronic filing system.

Where appropriate the email and the attachments can be printed out to be stored on a paper file, however, a printout does not capture all the audit information which storing the email in .msg format will.

Email text only
If the text in the body of the email requires filing, the same method can be used as that outlined above. This will retain information for audit trail purposes. Alternatively the email can be saved in .html or .txt format. This will save all the text in the email and a limited amount of the audit information. The email cannot be re-sent if it is saved in this format.

The technical details about how to undertake all of these functions are available in application Help functions.

How long to keep emails
Email that needs to be kept should be identified by content; for example, does it form part of a pupil record? Is it part of a contract? The retention for keeping these emails will then correspond with the GNSFC’s Record Management Policy. These emails must be saved into an appropriate electronic filing system or printed out and placed on paper files.

Social Media

Social Media – official use

- Expectations regarding safe and responsible use of social media will apply to all members of GNSFC and exist in order to safeguard both the setting and the wider community, on and offline. Examples of social media may include Facebook, Twitter, blogs, forums, bulletin boards, apps and others
- Official social media sites will be password protected and where appropriate, will be linked to GNSFC website
- Any online publication on official social media sites will comply with legal requirements including the Data Protection Act 1998, right to privacy conferred by the Human Rights Act 1998, or similar duty to protect private information and will not breach any common law duty of confidentiality, copyright etc.
- Members of staff participating in online activity as part of their capacity as an employee of GNSFC, are requested to be professional at all times and to be aware that they are an ambassador for GNSFC.
- Staff using social media officially will be responsible, credible, fair and honest at all times and consider how the information being published could be perceived or shared.
- Staff using social media officially will always act within the legal frameworks they would adhere to within the workplace, including libel, defamation, confidentiality, copyright, data protection as well as equalities laws.
- Staff using social media officially will be accountable and must not disclose information, make commitments or engage in activities on behalf of GNSFC unless they are authorised to do so.
- All communication between staff and members of the community on GNSFC business must take place via approved communication channels such as an official setting, provided email address or phone numbers
- Staff using social media officially will inform their Line Manager, the Designated Safeguarding Lead and/or the Headteacher of any concerns such as criticism or inappropriate content posted online.
- Staff will not engage with any direct or private messaging with children or parents/carers through social media and will communicate via official communication channels.
- Inappropriate use of social media during work hours or whilst using work devices may result in disciplinary or legal action and removal of Internet facilities.
- Any concerns regarding the online conduct of any member of staff on social media sites should be reported to the Headteacher or Business Manager and will be managed in accordance with policies such as allegations against staff, behaviour, staff handbook and safeguarding/child protection.

Social Media – personal use

- All members of GNSFC are advised not to publish specific and detailed private thoughts, concerns, pictures or messages on any social media services, especially content that may be considered threatening, hurtful or defamatory to others.
- All members of staff must not communicate any work-related matters via any personal social media sites, applications or profiles. Any pre-existing relationships or exceptions that may compromise this must be discussed with Designated Safeguarding Lead and/or the Headteacher.
- Information and content that staff members have access to as part of their employment, including photos and personal information about pupils and their family members, colleagues etc. will not be shared or discussed on personal social media sites.
- All members of staff are encouraged to carefully consider the information, including text and images, they share and post online and to ensure that their social media use is compatible with

their professional role and is in accordance with GNSFC policies (safeguarding, confidentiality, data protection etc.) and the wider professional and legal framework.

- Members of staff will notify the Headteacher or Business Manager immediately if they consider that any content shared or posted via any information and communications technology, including emails or social networking sites conflicts with their role in GNSFC setting.
- Members of staff are encouraged not to identify themselves as employees of GNSFC on their personal social networking accounts. This is to prevent information on these sites from being linked with GNSFC and also to safeguard the privacy of staff members and the wider community.
- Members of staff will ensure that they do not represent their personal views as that of GNSFC on social media.
- GNSFC email addresses will not be used for setting up personal social media accounts.

Policies and procedures

Staff are responsible for ensuring they are familiar with all relevant policies and procedures relating to E-Safety, Social Media and Emails. Key policies are:

- I.C.T Policy
- Data Protection Policy
- Records Management Policy
- Handling Data Subject Request Policy
- Privacy Notices (i. Parent/Carers, ii. Workforce iii. Governors/Volunteers)

These are available on the GNSFC intranet X: General/Centre/Policies and Procedures or a hard copy can be requested from Reception or the Business Manager.