DANESMEAD, FULFORD CROSS, YORK YO10 4PB
TEL: (01904) 654983

YORK STEINER SCHOOL

STAFF IT ACCEPTABLE USE POLICY

Approved by:	Board of Trustees	**Date:**	October 2021
Last reviewed on:	**October 2021**		
Next review due by:	October 2024		

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

This policy does not form part of any employee's terms and conditions of employment and is not intended to have contractual effect. It is provided as guidance for all members of staff at the School who are required to familiarise themselves and comply with its contents. The School reserves the right to amend its content at any time.

This policy outlines the standards that the School requires all users of these systems to observe, the circumstances in which the School will monitor use of these systems and the action the School will take in respect of any breaches of these standards.

The use by staff and monitoring by the School of its electronic communications systems is likely to involve the processing of personal data and is therefore regulated by the Data Protection Act 2018, together with the Employment Practices Data Protection Code issued by the Information Commissioner.

Staff are referred to the School's Data Protection Policy for further information. The School 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 UK 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 School's electronic systems from unauthorised access or harm. Breach of this policy will be regarded as a disciplinary offence and dealt with under the School's disciplinary procedure and in serious cases may be treated as gross misconduct leading to summary dismissal.

The School has the right to monitor all aspects of its systems, including data which is stored under the School's computer systems in compliance with the Data Protection Act 2018.

This policy mainly deals with the use (or misuse) of computer equipment, e-mail, internet connection, telephones, mobile devices including tablets and voicemail, but it applies equally to the use of fax machines, copiers, scanners, and the like.

Equipment Security and Passwords

All members of staff are responsible for the security of the equipment allocated to or used by them and must not allow it to be used by anyone other than in accordance with this policy.

Passwords are unique to each user and must be changed regularly to ensure confidentiality. Passwords should never be written down or stored online. Staff are required to select a password that cannot be easily broken and which contains at least 8 characters including both numbers and letters.

Passwords must be kept confidential and must not be made available to anyone else unless authorised by a School Manager who will liaise with the School HR/Admin Manager as appropriate and necessary. Any member of staff who discloses his or her password to another employee in the absence of express authorisation will be liable to disciplinary action under the School's Disciplinary Policy and Procedure. The School understands in rare or urgent circumstances, for example when a Staff member is off site or off sick, there may be a need to request their password for the purpose of unlocking School IT equipment that may be locked out for their sole use i.e. a laptop for general purpose use.

If given access to the School e-mail system or to the internet, staff are responsible for the security of their devices. Staff are required to log off when they are leaving the device unattended or when leaving the office to prevent unauthorised users accessing the system in their absence. The School Managers may do spot checks from time to time to ensure compliance with this requirement.

Staff should be aware that if they fail to log off and leave their terminals unattended they may be held responsible for another user's activities on their terminal in breach of this policy, the School's Data Protection Policy and/or the requirement for confidentiality in respect of certain information.

Logging off prevents another member of staff accessing the system in the user's absence and may help demonstrate in the event of a breach in the user's absence that they were not the party responsible.

Staff without authorisation should only be allowed to use terminals under supervision. Desktop PCs and cabling for telephones or computer equipment should not be moved or tampered with without first consulting and obtaining the express approval of the School HR/Admin Manager.

On the termination of employment for any reason, staff are required to provide details of their passwords and provide a full handover detailing the drives, folders and files where their work can be located and accessed. The School reserves the right to require employees to hand over all School data held in computer useable format.

Members of staff who have been issued with a laptop, mobile device or any other technology must ensure that it is kept secure at all times, especially when travelling. Passwords must be used to secure access to data kept on such equipment to ensure that confidential data is protected in the event that the machine is lost or stolen. Staff should also observe basic safety rules when using such equipment e.g. ensuring that they do not use or display such equipment in isolated or dangerous areas. Staff should also be fully aware that if using equipment on public transport documents can be easily read by other passengers.

Systems Use and Data Security

Members of staff should not delete, destroy or modify any of the School's existing systems, programs, information or data which could have the effect of harming or exposing to risk or harm the School's, its staff, students, or any other party.

All members of staff are prohibited from downloading, installing or running software from external sources without obtaining prior authorisation from the School HR/Admin Manager who will consider bona fide requests for work purposes. Please note that this includes instant messaging programs, screensavers, photos, video clips, games, music files and opening any documents or communications from unknown origins.

Where consent is given all files and data should always be virus checked before they are downloaded onto the School's systems. If in doubt, the employee should seek advice from the School HR/Admin Manager.

No device or equipment should be attached to our systems without the prior approval of the School HR/Admin Manager. This includes, but is not limited to, any mobile device, tablet, USB device, digital camera, MP3 player, infra-red connection device or any other device.

Staff should be cautious when opening emails from unknown external sources or where for any reason an email appears suspicious (such as ending in '.exe'). The School HR/Admin Manager should be informed immediately if a suspected virus is received. The School reserves the right

to block access to attachments to email for the purpose of effective use of the system and compliance with this policy. The School also reserves the right not to transmit any email message.

Staff should not attempt to gain access to unauthorised or restricted areas of the network or to any password-protected information unless they are specifically authorised to do so.

Misuse of the School's computer systems may result in disciplinary action up to and including summary dismissal. For further guidance on what constitutes misuse please see the section entitled *Inappropriate Use of the School's Systems and Guidance* under 'E-mail etiquette and content' below.

Email Etiquette and Content

Email is a vital business tool, but often lapses inappropriately into an informal means of communication and should therefore be used with great care and discipline. The School's email facility is intended to promote effective communication within the business on matters relating to the School's business activities and access to the School's e-mail facility is provided for work purposes only.

Staff are strictly prohibited from using the School's email facility for personal emails at any time and are reminded that the school has the right to monitor and access all areas of its systems.

Staff should always consider if email is the appropriate medium for a particular communication. The School encourages all members of staff to make direct contact with individuals rather than communicate by email 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 School'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. Staff are encouraged wherever practicable to write a draft email first, print it out and review it carefully before finalising and sending. As a rule of thumb if a member of staff would not be happy for the email to be read out in public or subjected to scrutiny then it should not be sent.

All members of staff should remember that emails 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 School. 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 School in the same way as the contents of letters or faxes.

E-mail messages may of course be disclosed in legal proceedings in the same way as paper documents. Deletion from a user's inbox or archives does not mean that an e-mail is obliterated and all e-mail messages should be treated as potentially retrievable, either from the main server or using specialist software. This should be borne in mind when considering whether e-mail is an appropriate forum of communication in the circumstances of the case and if so the content and language used.

Staff should assume that e-mail messages may be read by others including any person mentioned or otherwise identified in the content of the email 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 School standard disclaimer should always be used on every email.

Staff should ensure that they access their emails at least once every working day, stay in touch by remote access when travelling or working out of the office and should use an out of office response when away from the office for more than a day. Staff should endeavour to respond to emails marked 'high priority' as soon as is reasonably practicable.

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 a school manager immediately. If a recipient asks you to stop sending them personal messages then always stop immediately. Where appropriate, the sender of the email should be referred to this policy and asked to stop sending such material.

If you feel that you have been harassed or bullied, or are offended by material sent to you by a colleague via email, you should inform your manager who will usually seek to resolve the matter informally. You should refer to our Inclusion, Equality and Diversity Policy and the Anti-Harassment and Bullying Policy for further information and guidance.

If an informal procedure is unsuccessful, you may pursue the matter formally under the School's formal Grievance Procedure. Further information is contained in the School's Inclusion, Equality and Diversity Policy, Anti-Harassment and Bullying Policy and Grievance Policy and Procedure.

As General Guidance, Staff Must Not:

- Send any email, 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 private emails at work which they would not want a third party to read;
- Send or forward chain mail, junk mail, cartoons, jokes or gossip either within or outside the School;
- Contribute to system congestion by sending trivial messages or unnecessarily copying or forwarding emails 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;
- Download or email text, music and other content on the internet subject to copyright protection, unless it is clear that the owner of such works allows this;
- Send messages containing any reference to other individuals or any other business that may be construed as libellous;
- 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 School 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. 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 email which has been wrongly delivered should return it to the sender of the message. If the email 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. You should then inform your Manager, the Head Teacher or the School HR/Admin Manager as soon as is reasonably practicable.

Use of the Web and the Internet

When a website is visited, devices such as cookies, tags or web beacons may be employed to enable the site owner to identify and monitor visitors. If the website is an inappropriate one such a marker could be a source of embarrassment to the School, especially if a member of staff has accessed, downloaded, stored or forwarded inappropriate material from the website. Staff may even be committing a criminal offence if, for example, the material is pornographic in nature.

Staff must not therefore access from the School's system any web page or any files (whether documents, images or other) downloaded from the web which, on the widest meaning of those terms, could be regarded as illegal, offensive, in bad taste or immoral. While content may be legal in the UK it may be in sufficient bad taste to fall within this prohibition.

As a general rule, if any person within the School (whether intending to view the page or not) might be offended by the contents of a page, or if the fact that the School's software has accessed the page or file might be a source of embarrassment if made public, then viewing it will be a breach of this policy.

Staff should not under any circumstances use School systems to participate in any personal social media activity, internet group discussions, 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 School's website may be found at www.yorksteinerschool.org. 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 the School HR/Admin Manager or Marketing Executive in

the first instance. Only expressly authorised and designated members of staff are permitted to make changes to the website.

Inappropriate Use of Equipment and Systems

Access is granted to the web, telephones and to other electronic systems, for legitimate work purposes only.

Misuse or abuse of our telephone or e-mail system or inappropriate use of the internet in breach of this policy will be dealt with in accordance with the School's Disciplinary Policy and Procedure.

Misuse of the internet may, in certain circumstances, constitute a criminal offence. In particular, misuse of the e-mail system or inappropriate use of the internet by viewing, accessing, transmitting or downloading any of the following material, or using any of the following facilities, will amount to gross misconduct. Please note that this list is not exhaustive:

- Accessing pornographic material (that is writings, pictures, films or video clips of a sexually explicit or arousing nature), racist or other inappropriate or unlawful materials;
- transmitting a false and/or defamatory statement about any person or organisation;
- sending, receiving, downloading displaying or disseminating material which is discriminatory, offensive, derogatory or may cause offence and embarrassment or harass others;
- transmitting confidential information about the School and any of its staff, students or associated third parties;
- transmitting any other statement which is likely to create any liability, for either the employee or for the School (whether criminal or civil);
- downloading or disseminating material in breach of copyright;
- copying, downloading, storing or running any software without the express prior authorisation of the School HR/Admin Manager;
- engaging in online group chats, instant messaging, social networking sites and online gambling;
- forwarding electronic chain letters and other materials;
- accessing, downloading, storing, transmitting or running any material that presents or could present a risk of harm to a child.

Any such action will be treated very seriously and may result in disciplinary action up to and including summary dismissal.

The Head Teacher reserves the right to check staff devices if there are suspicions of misuse.

Where evidence of misuse is found the School 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.

Staff Protocol for use of Social Media

Where designated staff (admin managers of our social media sites and website) are posting on the School's own social media, website or in the press the following steps must be taken:

Ensure any children in photographs have permission to be photographed using the school's latest photo permission records. Ensure that there is no identifying information relating to any pupils in the post - for example any certificates in photos are blank/without names or the pupil'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 School or any achievements.

Protecting Reputation

Staff must not post disparaging or defamatory statements on school social media/the press or their own social media sites about:

- the School;
- current, past or prospective Staff;
- current, past or prospective pupils;
- parents, carers or families of;
- the School's suppliers and services providers; other affiliates and stakeholders; and
- Anyone they know through their association with the School.

Staff should also avoid social media communications that might be misconstrued in a way that could damage the School'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 School 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 anyone on the internet (including the School 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 School as a member of Staff whether past, current or prospective, they must also state that their views do not represent those of the School.

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/carers.

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

If a member of Staff is uncertain or concerned about the appropriateness of any statement or posting, they should refrain from making the communication until they have discussed it with the Administration Manager.

If a member of Staff sees content in social media that disparages or reflects poorly on the School, its Staff, pupils, parents/carers, service providers or stakeholders, they are required to report this in the first instance to the Administration Manager without unreasonable delay. All Staff are responsible for protecting the School's reputation.

Respecting Intellectual Property & Confidential Information:

Staff should not do anything to jeopardise School confidential information and intellectual property (e.g. the School logo) through the use of social media.

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

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

Staff must not create new social media pages containing the school name or any identifying logo, name or slogan connected to the school without explicit written consent from the Administration Manager.

To protect yourself and the School against liability for copyright infringement, please check that imagery has complete permission for public use (particularly when taken from books or the internet). Do not use if you are in any doubt. If 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 Administration Manager in the first instance before making the communication.

Respecting Colleagues, Pupils, Parents/Carers, Clients, Service Providers and Stakeholders

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

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