ELECTRONIC COMMUNICATIONS POLICY
Including Use of Social Networking Sites

Rationale

The use of electronic communications has grown considerably in recent years. The internet is one of the most popular sources of information whilst ease of use and speed has made email the most common form of communication between people. Social networking sites have made sharing and keeping in touch with others who are near or far away a quick and easy thing to be able to do. The advent of text messaging and smart phones now means many people can communicate easily away from a normal computer.

When used correctly, all forms of electronic communication provide an efficient way of sharing information. Correspondingly, incorrect or improper use will have the opposite result.

Electronic communications are developing at a fast rate. This policy encompasses what is relevant now and is not intended to be exhaustive. Methods of communication and devices will develop rapidly. Whatever the method of communication or the device it is made on, the rationale of this policy remains the same.

Any misuse of the systems may be regarded as a disciplinary offence.

Policy

This policy respects and complies with the applicable laws including (but not limited to):

- Telecommunications Act 1984
- Copyright, Designs & Patents Act 1988
- Computer Misuse Act 1990
- Disability Discrimination Acts & SENDA 1995
- Data Protection Act 1998
- General Data Protection Regulation (GDPR) 2018
- Human Rights Act 1998
- Regulation of Investigatory Powers Act 2000
- Telecommunications (Lawful Business Practice) Regulations 2000
- Telecommunications (Interception of Communications) Regulations 2000
- Freedom of Information Act 2000
- Electronic Communications Act 2000
- Communications Act 2003

No provision contained in the policy is intended to contradict or contravene such legislation. Neither is this policy meant to restrict legitimate and authorised educational activity.

All members of the school (including staff and students) must comply with this policy as set out below, and must be aware that the use of any school system is not entirely confidential. Use may be monitored (as described below) to ensure compliance with school policies and applicable legislation.

Guidelines

A breach of this policy may result in disciplinary action in accordance with the school's disciplinary procedure. In certain circumstances, e.g. using email to communicate obscene material, a breach of this policy may be considered to be gross misconduct resulting in dismissal.

School systems must not be used inappropriately. The following is an illustrative list of inappropriate use, but it is not intended to be exhaustive. Telephones, email and the internet, including social networking sites, must not be used for:

- Harassment or bullying – all communications should be consistent with the school's Equality policy
- Private commercial purposes
- Breaching copyright or confidentiality
- Intentional propagation of viruses
- Disrupting or damaging other systems by carrying out acts of a malicious or disruptive nature
- Excessive personal use
- Excessive use without due regard for the load this places on the school systems and the effect on other users, for example, downloading games to play against others across the internet or sending bulk emails (please refer to the advice at the back for further information).

Monitoring Use

The Regulation of Investigatory Powers Act does not allow the interception of communications by an employer unless the employer has "lawful authority". The Lawful Business Practice Regulations authorise monitoring for a number of purposes (listed below) and the school has selected the least intrusive methods of monitoring. While the school has no wish to interfere with the privacy of its members, it is required to discharge a number of legal duties that are laid down on all employers and managers of computer systems concerning what passes through, and is stored within, their systems – for example, to ensure that these are not used for criminal or other improper purposes, to prevent the spread of computer viruses, and to avoid other situations that might corrupt or degrade the operations of the school's computer systems or those of other systems elsewhere.

Thus, the school reserves the right to monitor telephone use, internet use, access email and other material on its computer systems from time to time for various reasonable and necessary purposes including those below:

- Checking compliance with all school regulations and policies
- Preventing or detecting crime
- Investigating or detecting unauthorised use
- Checking for viruses or other threats to the performance of the system
- Investigating abnormal system behaviour
- Resolving a user problem
- Monitoring standards of service or training
- Maintaining or carrying out school business.

Such monitoring will be kept to a reasonable minimum and every care will be taken to comply with all applicable data protection and privacy legislation in respect of the confidentiality of any

material that is monitored in so far as this does not conflict with duties laid down in other legislation or with the prevention of harassment or other serious breaches of the school's disciplinary procedures. Monitoring may include email and internet scanning software and software (eg Smartsync) to monitor use of PCs or laptops by students in lessons or at other times.

Individual emails will not be read by anyone except the sender or recipient if they are clearly marked as such. However, this will not be the case where access to the content of the email is required for the prevention or detection of a suspected crime or to prevent the inappropriate use of email as detailed in this policy.

Any investigation other than day-to-day monitoring requires the authority of the Principal or his/her nominee in order to take place. The person who grants the authority should be satisfied there are reasonable grounds for this request.

Personal Use

The personal use of email or the internet by staff or students is permitted providing that it is not excessive and does not interfere with the proper performance of that person's duties. It is good practice to maintain a distinction between what is a business email and what is a personal email, for example by marking personal emails as 'personal'.

The personal use of email and internet for students is permitted and it is acknowledged that use of these services is an integral part of study and engagement with the school and its staff. In general it is expected that the school based email system will be used for business purposes and personal emails will be conducted through home based accounts. Emails should not generally be accessed when staff are in a direct supervisory position, e.g. teaching a lesson.

Telephones, email and the internet must not be used to carry out private commercial activities. Personal telephone calls should be kept as brief as possible. Personal calls should not be made to non-geographic numbers (starting 084 or 087), mobile phones or overseas numbers without prior permission. The school must be reimbursed for the cost of the calls.

Internet Use

The internet is accessed via the school network all traffic must adhere to the ICT Acceptable Use Policy. Users should be aware of and comply with this policy.

Staff should note that personal use is a privilege and must not be excessive or interfere with the proper performance of an employee's duties.

The internet must not be used inappropriately. The following is an illustrative list of inappropriate use, but it is not intended to be exhaustive. The internet must not be used for:

- Accessing, downloading, storing recording or bookmarking sites that are offensive, obscene, defamatory, abusive or otherwise unlawful. (for instance, those that facilitate hacking or contain pornographic material)
- Publishing material that brings the school's reputation into disrepute.
- Downloading software which breaches the software company's rights or licence agreements.

Unfortunately the largely uncontrolled nature of the internet means that users can inadvertently access sites containing offensive, obscene, defamatory, abusive or otherwise unlawful material. In these instances users must exit such sites immediately. Prolonged or regular access to such sites is considered as intentional misuse of the facility.

The school provides laptops to many members of staff and the use of these away from the workplace is a recognised purpose of their issue. Staff should appreciate that the above guidance still applies while using a laptop out of school and where other people are allowed to use a school laptop, its use should be monitored by the member of staff. Staff should be conscious of what they store on a school laptop of a personal nature, e.g. photographs or other documents.

The school takes no responsibility for any online transactions and is not liable for the failure of security measures. All users should be aware that internet use may be recorded.

Email Use

In terms of the law, email communications are no different to any other form of written communication; they can be legally binding. Consequently they are, for instance, actionable within the laws of defamation and libel; they are recognised as being capable of contributing to harassment; and they can create or break contracts.

Emails frequently carry information about individuals (personal data) in the form of facts, intentions or opinions about individuals. Any emails produced in the course of school business that contain personal data must be managed in compliance with data protection legislation. This includes the right of individuals, including parents and carers, to request a copy of the data held about themselves on request.

With regards internal emails to all staff and all teaching staff there is an email protocol; the aim of this protocol is to reduce the number of internal emails as part of the school's workload reforms.

The email system is the property of the school but this does not alter the intellectual property rights in the work. Staff should note that personal use is a privilege and must not be excessive or interfere with the proper performance of an employee's duties.

The email system must not be used inappropriately. The following is an illustrative list of inappropriate use, but it is not intended to be exhaustive. Email must not be used for:

- Sending messages that are offensive, obscene, defamatory, abusive or otherwise unlawful. Emails, like any other form of written communication, can be used as evidence in a court of law
- Sending material that brings the school's reputation into disrepute
- Sending links to web pages or bulletin boards that are offensive, obscene, defamatory, abusive or otherwise unlawful (for instance, those that facilitate hacking or contain pornographic material)
- Sending unsolicited commercial or advertising material.

Unfortunately the largely uncontrolled nature of the internet means that email users can be identified remotely and streams of offensive advertising and other material directed to them, although they themselves may have taken no action to solicit this.

All email users are, therefore, asked to contribute to the monitoring and control of this nuisance by reporting the receipt of offensive email as promptly and fully as is reasonably practical, via the

relevant management chain (or as may from time to time be advised) in order to assist the school in taking steps to block the offending material.

All should be aware that deleting an email may not remove all instances of that message. There may be copies of the message elsewhere, for instance, the recipients system or back up files held on central servers.

Entitlement to access an individual's email account will normally automatically cease on the date on which an individual's relationship with the school has terminated. If additional access is required to an email account then this must be authorised by the Principal or his/her nominee in order to take place.

Social Networking Sites

The use of online social networking sites (e.g. Facebook, Twitter, YouTube, etc) has become a very significant part of life for many people. They provide a positive way to keep in touch with friends and colleagues, and can be used to exchange ideas and thoughts on common interests, both personal and work-related.

There have been occurrences where these services have been used for less positive reasons or used for an unreasonable length of time during working hours, hence the need for formal guidance.

If someone's personal internet presence does not make any reference to the school, its staff or students and the school cannot be identified (and this could include identification by other members of the school), the content is unlikely to be of concern to the school. If employment (staff) or membership (students) at the school is referred to then the information posted would need to comply with the conditions outlined below.

It should be noted that comments, photos and videos, etc, posted on social networking sites are often available to be viewed by anyone with internet access. Therefore, they are public and not private and depending on any individual account privacy settings can be freely viewed by anyone.

Where it is brought to the school's attention that there may be material on a social networking site that may be of concern to the school or one of its members, the school has a duty to investigate.

An individual is free to talk about the school. The right to 'freedom of speech' is often cited by students concerning their comments on social networking sites. In practice, the right to freedom of speech is not absolute in any country and the right is commonly subject to limitations, such as laws concerning libel, slander, obscenity, sedition, copyright violation and revelation of information that is classified or otherwise. Therefore the right to write or say what you like, about who you like, when you like, doesn't fully exist.

Sites should not be used to verbally abuse staff or students or bring the reputation of the school into disrepute. Privacy and feelings of others should be respected at all times. Staff members should obtain the permission of individuals before posting contact details or pictures. Care should be taken to avoid using language which could be deemed as offensive to others. Instances which contravene the above will be treated in the same way as if it was written on paper or spoken and subject to the same disciplinary procedures as appropriate. Instances where the school is brought into disrepute may constitute misconduct or gross misconduct and disciplinary action will be applied. Please refer to the relevant school disciplinary procedure.

If a member of staff wishes to initiate a school related social networking site permission must be sought from their line manager and their SLT link. Staff should keep personal and school based email addresses separate and for school based work, use their school based email address.

A member of staff should not disclose confidential information relating to his/her employment at the school.

If information on the site raises a cause for concern with regard to conflict of interest, staff members should raise the issue with their line manager.

If approached by a media contact about content on a site relating to the school, a member of staff should pass the matter onto a member of SLT.

Viewing and updating personal sites should not take place during working times, unless in exceptional circumstances, such as where activities form part of an educational project and this has been agreed in advance as appropriate by the line manager. Reasonable access is acceptable before/after working hours and during work breaks (although please be advised that if a computer screen is used throughout the day, employees are required to have regular breaks away from a screen).

Sites should not be used for accessing or sharing illegal content.

Any serious misuse of social networking sites that has a negative impact on the school may be regarded as a disciplinary offence.

The school does not discourage staff and students from using such sites. However, all should be aware that the school will take seriously any occasions where the services are used inappropriately. If occasions arise of what might be read to be online bullying or harassment, these will be dealt with in the same way as other such instances.

Information on the school's acceptable use of ICT can be found in the school's ICT Acceptable Use Policy. There are versions for both staff and students.

Text Messages

Text messages are a useful way to communicate small messages or information quickly and in bulk that may not require a response from the recipient(s).

The school subscribes to an internet based service that enables bulk text messages (and phone messages and emails) to parents and staff. This is primarily intended to share information (such as school closures through snow) or reminders (such as forthcoming parents' evenings).

Staff should not use personal phones to send or receive text messages from students. School based phones are available if needed.

Messages must not be offensive, obscene, defamatory, abusive or otherwise unlawful. A text message, like any other form of written communication, can be used as evidence in a court of law. Messages must not bring the school's reputation into disrepute.

Use of Cameras, Video Recorders, Phones or Other Devices with a Recording Facility

The use of cameras, video recorders, phones or other devices with a recording facility in lessons can enhance learning and the use of multimedia facilities forms an important part of the school's curriculum.

Many faculties and subject areas in the school have purchased cameras or video recorders with the purpose that they are used as part of the curriculum.

Where a 6th form student wishes to use their own device as part of the lesson, they must obtain the supervising member of staff's permission first and understand the remit under which they are being allowed to use it. Unauthorised use of phones or other devices in lessons is forbidden. Students in Years 9 to 11 are not permitted to use mobile phones during or between lessons.

Be aware that some students may have opted out of the consent for them to be photographed or filmed.

Raising Awareness of the School's Electronic Communications Policy

The school will endeavour to raise awareness of the issues surrounding electronic communications through a variety of methods.

It will look at, amongst others, the importance of eSafety, Cyberbullying, use of social networking sites and the use of mobile phones or other devices in school through means such as specific lessons, the ICT curriculum (or other subject areas, as appropriate), assemblies and posters.

Key Points of Advice Concerning Electronic Communications

- Write all email messages in a professional manner. The content of an email should be to the same standard as a letter
- When sending emails to parents use the 'Bcc' feature of an email to ensure data protection is respected
- Check carefully when doing a 'reply all' to an email about who the recipients are
- Consider carefully the full implications of sending bulk emails (emails to large numbers of recipients). For example, a 5MB email sent to 200 staff could consume 1000Mb of server disk space
- Try and minimize the size of emails and their attachments. For example, large photos can often be made much smaller before being emailed
- Consider the use of servers (eg staff files) to publish and share documents and pictures and then circulate the address in your email message rather than use large attachments
- Be careful when sending emails containing personal or confidential information. Check the recipient's name, especially if there is more than one person with the same name
- Avoid sending sensitive information in an email. Sending an email is like sending a postcard through the post
- Try to minimize the use of graphics, different fonts, formats stored within a document when sending it as an attachment to an email
- Do not open attachments from unknown sources. Always virus scan a document received as an attachment in an email before opening the document
- The receipt of any email communication containing obscene material must be reported immediately to either your line manager, a member of SLT or an IT technician

- Emails should not be accepted if they contain inappropriate language and/or content. They should be returned immediately to the sender with a request for a revised version to be submitted. If appropriate, your line manager, member of SLT or an IT technician should be informed
- You should endeavour to ensure that personal email cannot be interpreted as official school correspondence
- Avoid using continuous uppercase text unless for particular emphasis, as this is interpreted as 'shouting'
- Be careful when using humour or sarcasm within a message as this can be easily misinterpreted
- Try to save emails within a meaningful file structure and delete messages periodically.

Monitoring, Evaluation and Review

The policy will be monitored, evaluated and reviewed every three years by the senior leadership team.

Dissemination of the Policy

This policy is available on the school website, on request to parents and carers, the LA and Ofsted through the Principal.

Date approved by the governing body	Feb 2020
Date for review	Feb 2023