Electronic Communication Guidance for Staff

Approved By: The IMB

Version: 1.0

Created on: February 2023

Amended on:

Next review date: February 2024

Contents

- 1. Introduction
- 2. Safe and responsible use of:
- 2.1 Internet
- 2.2 Email
- 2.3 Online social communications

2.4 Real time communication e.g. text messaging, web camera, VC, mobile phone

3. Misuse of electronic equipment

- 4. Monitoring and privacy
- 5. Breaches and sanctions

1. Introduction

This guidance is provided to ensure that electronic communication systems are used responsibly and safely at all times by staff and IMB members. It is also the intention that the guidance, if followed, will protect staff from any negative consequences arising from the use of electronic communication equipment. There are potentially negative implications for individuals and The Springfield Centre as a whole if the guidance is not followed.

This document is part of the school's Acceptable Use agreement.

Electronic communications equipment includes any device which allows text, voice, image or video communication. Examples include telephone, voicemail, computers, laptops, tablets, mobile and smartphones, digital cameras, web cameras and video cameras. Types of communication can include (but is not limited to) internet, telephone, email, text messaging, multimedia messaging, transmission of photographs and videos, contact via websites and social networking sites, blogging, wikis, contact via web cameras and internet phones, communication via tablet or smartphone apps.

Staff, IMB members will sign the school Acceptable Use Agreement to show they have understood and accepted the contents of this document.

2. Safe and Responsible use

2.1 The internet

The internet is a valuable work resource, which enriches teaching and learning. In school hours, staff are expected to restrict internet access to work related activities.

Staff must not use The Springfield Centre equipment or systems for any form of illegal activity, e.g. downloading copyrighted material, introducing a virus, hacking into other computers, viewing or downloading pornographic, obscene, offensive or any other inappropriate material from any source, transmitting or storing such material on a computer. Criminal proceedings may result if any equipment is used for illegal activity, regardless of whether it is personal or school owned.

Action you must take if you inadvertently access inappropriate material

Anyone inadvertently accessing inappropriate material should immediately inform the Designated Safeguarding Lead and ensure that the incident is recorded and identified to the Senior Leadership Team.

2.2 Email

All work-related emails should be written using a The Springfield Centre email address. The Springfield Centre email should be regarded as an official communication. Emails should be written in the same professional tone and text as any other form of official school communication.

Email is governed by the same rules which cover all professional correspondence. Therefore, copies should be kept as a record of the communication.

The Springfield Centre email accounts must not be used to send, store or circulate personal email.

The sending of abusive, threatening, discriminatory or other offensive email is forbidden and may be considered a criminal act. Bear in mind that emails may be submitted as evidence in legal proceedings and that email discussions with third parties can constitute a legally binding contract.

Email attachments should be opened with care unless you have absolute confidence in its origin as this is one of the most likely points of introducing a virus into a computer system.

An individual should not access the email of another individual within The Springfield Centre without express permission of the account holder or senior leader and a clear understanding of the reason for the proxy access. However, staff should be aware that The Springfield Centre email accounts may be accessed by other school staff for monitoring or management purposes as described in section 4.

Action you must take if in receipt of inappropriate emails

- It is impossible to control what information is sent to a member of staff by email. However, if offensive, obscene and/or discriminatory material is received it is then the responsibility of the receiver to report immediately, and in writing, to the Designated Safeguarding Lead. Never send a reply.
- Forward a copy of the email to the designated Safeguarding Lead. Ensure that the sender's information is also recorded as their email service provider may take action.
- However, do not forward any email containing a 'sexting' image of a child, even for investigation purposes. It is illegal to distribute indecent images of children, even if the image was originally created by the child themselves.

2.3 Online social communication

Many staff and pupils use social media for communication outside school. Staff should not use The Springfield Centre facilities to access or update personal social networks. Staff should be aware of the potential risk to their professional reputation and potential for safeguarding allegations caused by adding pupils, parents or friends of pupils to their social network contacts and are strongly recommended not to do so.

Care should be taken that comments made on a social network site, website or app do not relate to or identify the school, staff or pupils as this could result in disciplinary action (please refer to The Springfield Centre Social Media Policy).

It is recognised that online social communications tools, such as blogs and wikis, have a potentially useful role in education – such as on The Springfield Centre websites, learning journals, celebrating good work, sharing information and facilitating collaboration. Where pupils and their families are sharing these tools with staff in school it is important that this should always be through a school-based resource, such as the school's Learning Platform, using a The Springfield Centre account where all communication is open and transparent.

If a member of staff keeps a personal blog the content must maintain acceptable professional standards. Any inappropriate use may lead to disciplinary action in accordance with The Springfield Centre policy. All blogs should contain a disclaimer that the views expressed are personal and not necessarily those of the school or The Springfield Centre.

Schools are vulnerable to material being posted about them online and all staff should report this should they become aware of anything bringing the school into disrepute. The Springfield Centre staff or The Springfield Centre IT provider will regularly check using a search engine whether any such material has been posted.

Action you must take if you discover inappropriate, threatening or malicious material online concerning yourself or your school/The Springfield Centre • Secure and preserve any evidence. For example, note the web address

(URL) or take a screen shot or copy and print the screen

- Report immediately to your line manager, who will ensure the incident Is investigated
- After investigation, contact the uploader of the material or the Internet Service Provider/ website administrator and ask for the material to be removed.
 All social network sites have the means to report unacceptable material or activity on their site – some more readily available than others. If the material has been created by a pupil or staff member then the school have a responsibility to deal with it. Illegal material which is discrimination, hate crime or a credible threat of violence needs to be reported to the police.

2.4 Real time online communication (e.g Teams)

The ability to communicate using voice, text or webcams in real time using the computer, tablet devices, mobile phones and gaming machines makes these an excellent tool for a range of educational purposes, particularly during periods of partial closure. However, staff should take the same level of care with these tools as they would if working in a face to face situation with a pupil or group of pupils. Access should always be through a The Springfield Centre created account, never a personal account and it should be focused on a clearly specified educational objective.

There may be times when this kind of activity will happen outside normal school hours and off the school premises e.g. from a member of staff's home. In this situation, it should always be carried out with the full knowledge and agreement of a line manager. Staff should be aware that they must remain focused on the educational purpose of the communication and never allow it to become a social exchange. Staff should also agree to specific times for availability and only allow contact during these times, to protect their personal time. When a web camera is used it should have a clear purpose. Staff should be aware of the ability of meetings of this kind to be recorded without their knowledge. However, they may wish to use this function for their own security, as long as all parties are informed that recording is taking place.

Staff must protect their privacy by never allowing pupils or parents to obtain their personal contact details such as a mobile phone number or email address. Online bullying of staff by pupils is possible by mobile phone or email.

Action you must take if an incident occurs

- Report immediately and in writing to your line manager.
- Don't reply to abusive or worrying text or video messages.
- Don't delete messages. Keep them for evidence.
- Try and obtain the phone number if you can. Most calls can be traced.
- Report it to your phone provider and/or request a change of number
- Technical staff may also be able to help you to find or preserve evidence e.g. logs of the call.

3. Misuse of electronic equipment

Misuse is a disciplinary offence. Employees MUST NOT use The Springfield Centre equipment (including a school provided laptop/phone/PC/tablet) to:

- Store, view, download or distribute material that is obscene, offensive, pornographic, contains violent images, incites criminal behaviour or incites hatred of any person or group of people on the grounds of race, religion, age, gender, sexual orientation, disability or other protected characteristic
- Gamble
- Undertake political lobbying
- Promote or run a commercial business
- Download or distribute games, music or pictures from the internet for personal use (they can bring viruses with them, use up capacity on the servers and potentially breach copyright)
- Spend work time on personal matters (for example, arranging a holiday, shopping, looking at personal interest websites)
- Store any personal information on equipment or The Springfield Centre servers, including photos, videos and documents
- Send personal emails, texts or messages
- Publish anything on a website, social networking site or blog, which:
 - is critical about members of the school community including pupils
 - contain specific or implied comments you would not say in person
 - contain inappropriate comments which could cause offence or harassment on the grounds of gender, race, disability, age, religion or sexual orientation
 - have originated from a chain or joke email
- Conduct private and intimate relationships via The Springfield Centre systems
- Download or copy software (excluding software updates or educational use) or use the email system to transmit any documents or software without checking copyright or licence agreement

- Install software licensed to The Springfield Centre on a personal computer unless permission to do so is explicitly covered by the school licence agreement.
- Take, transmit or publish pictures of a member of staff or pupil on a mobile phone, camcorder or camera without the person's permission
- Give away email contact lists for non-school business. If in doubt, ask your line manager
- Access personal social media accounts or use online communication tools for personal communications during work time

Additionally, employees MUST NOT:

• Do anything which brings The Springfield Centre into disrepute

A personal laptop, phone, tablet or other equipment brought onto The Springfield Centre premises MUST NOT be used to undertake any of the above activities during the school day, nor should it have information stored within it which would be deemed to be unacceptable on a The Springfield Centre device. It is recommended that a personal laptop used in The Springfield Centre buildings should have a separate secure account for The Springfield Centre use. Additionally, a personal laptop used for any The Springfield Centre activity must be fully protected against virus infection.

4. Monitoring and Privacy

The Springfield Centre's email, Google docs/drive, website and internet facilities are business systems, owned by the school. The Springfield Centre also uses the following systems extensively but these are not owned by The Springfield Centre, these include: Integris and CPOMs. The school therefore reserves the right to monitor all use of the internet and of the school's IT systems. Usage will be monitored to ensure that the systems are being employed primarily for business and educational reasons, that there is no harassment or defamation taking place and that employees are not entering into illegal transactions. The Springfield Centre and personal electronic equipment on The Springfield Centre site may be examined if it is felt necessary to do so for Child Protection or potential disciplinary purposes.

Staff need to be aware that internet sites visited are traceable, and that deleted or trashed messages or attachments can be recovered.

Email, telephone calls and internal and external post (unless clearly identified as private and confidential post) should be used for business and educational reasons. To ensure this, monitoring can be carried out on a regular basis. The Springfield Centre leadership teams and technicians have access to all the school communication systems for monitoring and interception of communications in order to deal with matters in an employee's absence for illness or other reasons.

Any material stored on the school network or being circulated via the school email system has no rights of individual privacy. In accordance with Regulation of Investigatory Powers Act 2016 monitoring or surveillance without an employee's knowledge can be carried out on internal email systems, or information stored on a server. It is permitted to intercept communications in this way so the school can ensure its systems are being used properly in accordance with policies and are working correctly.

5. Breaches and Sanctions

Failure to follow any aspect of this guidance (either deliberately or accidentally) could lead to disciplinary action against staff in accordance with the school disciplinary policy, which may result in dismissal.

Please note this guidance is to be read in conjunction with the Acceptable Use Agreement for Staff, sent under separate cover.

Appendix 1

WHATSAPP GROUPS EMERGENCY CONTACT

The Springfield Centre plans to trial and create a WhatsApp group for all employees as a method of ensuring good communication. WhatsApp is a very commonly used online messaging service that a number of employees are already using on their phones or tablets. The app is very useful and effective for quickly messaging within a group of people.

The aim of the group is to ensure that we can contact all employees quickly as we are aware that email access may be limited. This sets out why and how we plan to implement the WhatsApp groups safely and seek your consent for you to join the group. However, the primary source of The Springfield Centre organisation & logistics will be via email. It is intended that WhatsApp will only be used as a back-up or when last minute changes occur, or when we want to make you aware of an important email (health and safety, emergency situations, snow days, etc.).

It's important to note that this group should ONLY be used for organisational purposes and not for any other reason.

What will we use The Springfield Centre WhatsApp groups for? (The below is not exhaustive):

School Closure, Invacuation Procedures (Lockdown), Urgent contact.

What we won't use it for? (The below is not exhaustive):

As a main method of contact

Non-urgent messaging