الإمـــارات
The Emirates

We track Your Child's Future
al ameer
English School

نمهد لمستقبل أولادكم
الأمـــيـــر
مدرسة الإنجليزية

Electronic Communications Guidance for School Staff

Updated January 2021

Contents

1. Introduction

This guidance is provided to protect Al Ameer School staff from harassment, real or alleged misuse and any consequential disciplinary action arising from the use of electronic communication equipment in or outside school. It is also intended to ensure that the school's equipment is used responsibly and safely at all times. There are implications for the actions of individuals and the school as a whole.

This document is part of the school's Online Safety Policy and Acceptable Use agreements.

Electronic communications equipment includes any device which allows text, voice, image or video communication. Examples include telephone, fax, voicemail, computer, laptops, tablets, mobile and smart phones, photocopier, digital cameras, web cameras, videos and palm-held equipment. 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 smart phone Apps.

Staff will sign the school Acceptable Use Policy to show they have understood and accept the contents of this document.

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

The internet

The internet is a valuable work resource, which enriches teaching and learning. In schools hours staff are expected to restrict internet access to work related activities. Reasonable personal use may be permitted outside recorded working time.

Staff must not use electronic equipment 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 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 Supervisor or Online Safety Leader in school and ensure that the incident is recorded in the online safety incident log.

Email

Staff should keep personal and school based email addresses separate and for school based work, use their school based email address.

All work-related emails should be written using a school email address. School 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 home-school correspondence. Therefore, copies should be kept as a record of the communication e.g. by keeping a saved or printed copy, forwarding the email to the school office or other relevant staff.

School 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 school without express permission and a clear understanding of the reason for the proxy access. However, staff should be aware that school 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 person in school (OSL) or the Principal. Never send a reply.

- Keep a printed copy of the email as evidence and pass a copy of the email to the appropriate person for the record. Ensure that the sender's information is also recorded as their email service provider may take action.

- 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.

Online social communication

Many staff and students use social media for communication outside school. Staff should not use school 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/students, parents or friends of pupils/students to their social network contacts and are strongly recommended not to do so. Staffs must not follow students online social media accounts

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

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. It is also important that photographs and descriptions of activities in the personal life of staff do not adversely affect the professional reputation of staff or the school. Staff should be aware that even if they have used the privacy settings, they may not be able to prevent material becoming public due to the risk of republishing by someone else.

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 school policy. All blogs should contain a disclaimer that the views expressed are personal and not necessarily those of the school .

Action you must take if you discover inappropriate, threatening or malicious material online concerning yourself or your school

- 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 OSL, who will investigate the incident

- 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.

Real time online communication

The ability to communicate using voice, text or webcams in real time using the computer, tablet devices and mobile phones makes these an excellent tool for a range of educational purposes. 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/student or group of pupils/students. Access should always be through a school 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. In this situation it should always be carried out with the full knowledge and agreement Supervisors. 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 Supervisors or OSL.
- 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 can be a serious disciplinary offence. Employees **MUST NOT** use school equipment (including a school provided laptop) 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 or disability
- 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 school time on personal matters (for example, arranging a holiday, shopping, looking at personal interest websites)
- Store personal information on the school network that uses up capacity and slows down the system (for example, personal photos, screensavers or wallpaper)
- Send emails, texts or messages or 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 school 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 school 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/Head Teacher
- 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 school into disrepute

A **personal laptop** brought onto the school 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 school device. It is recommended that a personal laptop used at school should have a separate secure account for school use. Additionally a personal laptop used for any school activity must be fully protected against virus infection.

4.Monitoring and Privacy

The school's email and internet facilities are business systems, owned by the school. 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. Electronic equipment on the school site may be search and examined.

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 primarily for business and educational reasons. To ensure this, monitoring can be carried out on a regular basis. School managers 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. 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 policy (either deliberately or accidentally) could lead to disciplinary action against staff in accordance with the school disciplinary policy, which may result in dismissal.

6.Good practice guidance for school staff

Pay close attention to the list of misuses in section 3 because this list is for your protection and clarifies how possible disciplinary action can be avoided.

In communications with pupils and parents, never give out personal information which identifies your home address, phone number, mobile phone number or personal email address. Once such information is known you are open to harassment through unwanted phone calls, text messages and emails.

Protect your social network site by using the correct privacy settings. Make sure that personal information cannot be seen from the links to your friends' sites.

Do not accept pupils as friends on your personal social network site. If at all possible do not include parents as friends.

Avoid the use of chat rooms, instant messaging or other social networking services which are accessed socially by pupils and are not monitored by the school.

Always keep a copy of email communications with pupils and parents (whether sent or received) and keep a note of the dates, times and content of telephone conversations.

If your school laptop is used outside school for non-school activities then set up a different user account to ensure that personal or confidential data is protected. Use a strong password to protect the school laptop from unauthorised access.

Make sure you do not allow people to see personal or confidential school information when a computer is left unattended. Turn it off, log off and set up a password-protected screen saver to prevent unauthorised access.

Keep all passwords and login details strictly private and always remember to log off correctly after using the computer. Never allow anyone else to use your personal login detail as you will then be held responsible for their online activity .

Always use the school's digital camera or video camera for taking school related pictures and upload them onto a school computer. Once uploaded, the images should be deleted from the camera's memory. Photographs of children should not be taken home to use on a personal computer.

If you are using school electronic equipment off site then take the same level of care as you would in school. A digital camera taken off site should not be returned to school with personal photographs on it.

It is not recommended that personal financial transactions are made on school equipment as information may become accessible to pupils.

Observe sensible precautions when taking photographs which may include pupils: always obtain students and/or parental permission if the photograph is for use on the school web site or Face book

Report immediately, and in writing, to the designated person in school (or your Principal) any web pages accessed or emails received where the content could be described as inappropriate or malicious. Keep copies as evidence.

7. Internal Communication – to Staff

- Time-Sensitive, Communications of High Importance – From time to time an important and urgent message may need to be relayed to staff. In this case the communication must be made as a face-to face communication, or if to a wider audience by means of Zoom/Google meet .
- Non-Time-Sensitive Communications of High Importance – If the communication is not time sensitive it should be sent by school Email which ensures a lasting record of the communication made for reference.
- Communications of Low to Medium Importance – These may be made by school Email or face-to-face depending on the circumstances and how many staff need to receive the communication.
- Communications Involving Sensitive Data – Most importantly, these should be kept to a 'Need to Know' basis. Previous points apply, however, only specifically relevant staff should receive the communication, and face-to-face communications are preferred.
- As per the 'Acceptable Use of Technology Policy', staff should never share logins and/or passwords to computer accounts, Email accounts or their mobile phones.
- A staff meeting is held on weekly basis. At times this is a whole staff meeting, at times departmental; staff are notified .
- Staff should check Emails regularly; at least twice daily including first hour before teaching.
- Staff should attempt to respond to Emails when required timely, notwithstanding the fact that they should not compromise their teaching to do so unless imperative.
- When sending Emails information should be kept as concise as possible with links or attachments made available if expansion on points is thought useful.

8. 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 Supervisor, a member of OSG 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 Supervisor, member of OSG 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 interpretedas '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.