Ysgol Uwchradd Y Frenhines Elisabeth
Queen Elizabeth High School

Moving Forward Together

ELECTRONIC COMMUNICATIONS POLICY

Date established by Governing Body: 6th December 2017

Responsible Person – Mrs S O'Kelly

Designated role – Assistant Head Teacher

Chair of Governors signature – Helen Starkey

Date - 06/12/2017

Policy Version Control

Version	Date	Page	Section	Reason for review	Summary of amendment	Chair of Governor's signature
1	6/12/17			New AHT appointed with responsibility for this policy		Helen Starkey 06/12/2017

- **Contents**

- **1. Introduction**

- First and foremost this policy is provided to protect both school staff and pupils 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 E Safety Policy and Acceptable Use Agreements.

- Electronic communications equipment includes (but may not be limited to) telephone, fax, voicemail, computer, laptops, tablets, mobile phones (all types), photocopier, digital cameras, web cameras, videos and palm-held equipment. Types of communication can include (but may not be limited to), internet, phone calls, email, text messaging, multimedia messaging, transmission of photographs and moving pictures, contact via websites and social network sites, blogging, wikis, contact via web cameras and internet phones.

- In agreeing to the Acceptable Use Policy when logging on to the school computer system, you are confirming acceptance of the contents of this document.

- This document relates to all teacher-pupil communication and communication between staff and external bodies, not just those conducted in school or using school equipment

- This document augments the EWC 'Code of Professional Conduct and Practice for Registered Teachers'
- **Failure to follow any aspect of this policy (either deliberately or accidentally) could lead to disciplinary action against you in accordance with the school's Disciplinary Policy which may result in dismissal.**

- **2. Safe and Responsible use of:**
  - **2.1 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 (for example at lunchtime).
  - Staff must not use electronic equipment for any form of illegal activity, e.g. downloading copyright material, introducing viruses, 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 the equipment used for illegal activity is personal or school owned.
  - **Action you must take if you inadvertently access inappropriate material**
  - Anyone inadvertently accessing inappropriate material should immediately inform the Head teacher or line manager in school and ensure that the incident is recorded.
  - **2.2 Email**
  - 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 racially abusive 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 not be opened 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 (or the head teacher). Never send a reply.

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

- **2.3 Online social communication such as Social Networks, Blogs**
- Many staff and students use the computer for social communication outside school. (e.g. Facebook) **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 of adding parents or friends of students as 'friends' on their social network site and are strongly recommended not to do so. Staff should not add pupils as friends to any social media accounts.
- Care should be taken that comments made on a social network site or blog 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 from 'friends' sites.

- It is recognised that online social communications tools, such as blogs and Wikis, have a potentially useful role in schools – such as on school 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 provision, such as the school Learning Platform, using a school log-in where all communication is open and transparent.
- If staff keep 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.

- The school is vulnerable to material being posted about them online and all staff should be aware of the need to report this should they become aware of anything bringing the school into disrepute.

- Twitter feeds offer a highly effective means of communication. Any departments or member of staff wishing to establish a school based twitter feed must seek the permission of the Headteacher prior to doing so.

- **Action you should 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 line manager or head teacher

- The school should endeavour to contact the uploader of the material or the Internet Service Provider/site 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 has a responsibility to deal with it.*

- **2.4 Real time online communication e.g. texting, using web cameras, chat, mobile phone**

- The ability to communicate in real time using the computer and other electronic devices (such as 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 student or group of 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 are likely to 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 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 contact details such as a mobile phone number or login details. Cyber bullying of staff by pupils is very common 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.
    - Use 1471 to try and obtain the 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. The following examples of misuse apply to all employees.

- 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 racial hatred
  - 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). This may be treated as fraud.
  - 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 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 letter
  - Conduct private and/or intimate relationships via school systems
  - Download or copy software (excluding software updates) 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
  - Make available to others email lists for non-school business. If in doubt, ask your line manager/Head teacher
  - Use internet chat rooms (other than the secure, moderated facilities which are provided within the school's Learning Platform)

- 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 machine. 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, which is the responsibility of the school. The school therefore reserves the right to monitor all use of the internet and of the school's ICT 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 searched and examined.
- Staff need to be aware that internet sites visited are traceable, and that deleted messages or attachments can be recovered.

- Email, telephone calls and internal and external post (unless clearly identified as private and confidential) should be used primarily for business and educational reason. To ensure this, monitoring can be carried out on a regular basis. School managers have proxy access to all the school's 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's network or being circulated via the school's email system has no rights of individual privacy. In accordance with RIPA (Regulation of Investigatory Powers Act 2000) 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 school 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's 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 and friends of pupils 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

- 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.

- The use of hand held walkie talkies is increasing in schools. Staff using this equipment should speak professionally and respect confidentiality. Be aware that the message could be overheard at either end

- 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 and make sure that individual pupils cannot be identified by name, especially if the photograph is for use on the school web site or Virtual Learning Environment (VLE).

- Report immediately, and in writing, to an appropriate person in school (e.g senior teacher or the head teacher) any web pages accessed or emails received where the content could be described as inappropriate or malicious. Keep copies as evidence.

- **7. Staff expectations of the school**

In order to ensure safe practice for staff, the school will:

- Enforce policies to protect staff and pupils from malicious use of mobile phones, in particular the use of camera and video functions on phones
- Ensure that the school's policy and procedures for home-school communication are shared with all staff
- Establish whole school systems for: storing emails, dealing with inappropriate messages and breaches of security
- Provide all staff with a personal email address to be used for all school-related communications.
- Establish a clear school policy for monitoring use of the school's electronic equipment by staff, including procedures for accessing email and files when staff are absent due to holiday, illness, etc
- Provide digital cameras and mobile phones which can be borrowed by staff as required for all school-related work
- Provide a safe learning environment, such as a VLE, for electronic communications with pupils
- Ensure there are established systems for reporting unwanted or accidental electronic communications and that staff know who the correct person to report any issues to is. Ensure these are correctly recorded. Treat such incidents seriously.
- Create procedures to regularly check the schools presence on the web to ensure material detrimental to the school is identified quickly.