Ysgol Uwchradd Y Frenhines Elisabeth
Queen Elizabeth High School

Moving Forward Together

Online Safety and Communications Policy

Date Established by Governing body: 3rd February 2021

Curriculum, Staffing & Pastoral Committee

Responsible Person – Miss Bethan Jones

Designated role – Assistant Headteacher

Chair of Governors signature – Helen Starkey

Review Date – Spring Term 2024

Policy Version Control

Version	Date	Page	Section	Reason for review	Summary of amendments	Chair of Governor's Signature
1	3/2/2021				New Policy to reflect change in practice.	Helen Starkey 3/2/2021

Contents:

Introduction

This policy applies to all members of QEHS (including staff, students, volunteers, parents/ carers, visitors, community users) who have access to and are users of QEHS ICT systems, both in and out of the school.

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. In addition, the policy is in place to educate pupils, staff, parents and the wider community about online safety.

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. (Appendix 1)

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'.

QEHS will deal with such incidents within this policy and associated policies for behaviour, anti- bullying and safeguarding and will, where known, inform parents/carers of incidents of inappropriate online behaviour that take place in and out of school.

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.

Schedule for Development/Monitoring/Review

Monitoring of the Online Safety and Communications Policy will take place at regular intervals.

The Governing Body will receive a regular report on safeguarding, including online safety.

The Online Safety and Communications Policy will be reviewed in the light of any significant new developments in the use of the technologies, new threats to Online Safety or incidents that have taken place.

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited)
- Internal monitoring data for network activity
- 360 safe self-evaluation tool

Roles and Responsibilities

The following section outlines the online safety and communication roles and responsibilities of individuals and groups within QEHS.

Governors are responsible for the approval of the Online Safety and Communications Policy and for its review. Monitoring of the effectiveness of this policy will be undertaken via regular feedback on online use, training and safeguarding. The Safeguarding link Governor will review Online Safety as part of their remit.

Headteacher and Senior Leaders:

- The Assistant Headteacher (AHT) has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the DCF Co-ordinator.
- The AHT should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff (*see flow chart on dealing with online safety incidents – included in a later section – "Responding to incidents of misuse" and relevant Local Authority HR / other relevant body disciplinary procedures*)
- The AHT IS responsible for ensuring that the DCF Coordinator and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The AHT will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The AHT will receive regular monitoring reports from the IT Manager.

DCF Coordinator/Designated Senior Person:

- Leads on online safety issues
- Takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies/documents
- Ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- Provides training and advice for staff
- Liaises with the Local Authority/relevant body
- Liaises with school technical staff
- Receives reports of online safety incidents and creates a log of incidents to inform future online safety developments
- Attends relevant meeting/committee of Governors
- Reports regularly to Senior Leadership Team
- Reviews and self-evaluates progress with 360 safe

IT Manager:

The Network Manager is responsible for ensuring:

- That the school's technical infrastructure is secure and is not open to misuse or malicious attack.
- That the school meets required Online Safety technical requirements and any Local Authority/other relevant body Online Safety Policy/Guidance that may apply.
- That users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed.
- That they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant.
- That the use of the network, internet, Virtual Learning Environment, remote access, email is regularly monitored in order that any misuse/attempted misuse can be reported to the AHT and/or Headteacher for investigation, action and/or sanction.
- That monitoring software/systems are implemented and updated as agreed in school policies.

Teaching and Support Staff:

Teaching and Support Staff are responsible for ensuring that:

- They have an up to date awareness of online safety matters and of the current school online safety policy and practices.
- They have read, understood and comply with the Staff Acceptable Use Agreement.
- They report any suspected misuse or problem to the Headteacher and/or AHT for investigation, action and/or sanction.
- All digital communications with students/parents/carers should be on a professional level and only carried out using official school systems.
- Online safety issues are embedded in all aspects of the curriculum through DCF, ICT and PSE and other activities.
- They monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices.
- In lessons where internet use is pre-planned students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- They abide by all guidelines linked to communication with regards to safe and responsible use. (Page 14-19 in policy)

Designated Senior Person for Child Protection:

The DSP should be trained in online safety issues and be aware of the potential for serious child protection/safeguarding issues to arise from:

- Sharing of personal data
- Access to illegal/inappropriate materials
- Inappropriate online contact with adults/strangers
- Potential or actual incidents of grooming
- Cyber-bullying
- The DSP should ensure that online safety is reflected in the safeguarding policy (See Safeguarding policy)

Students:

- Are responsible for using the school digital technology systems in accordance with the Student Acceptable Use Agreement (See BYOD consent and Appendix 1).
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations that are taught through ICT and DCF.
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Should understand the importance of adopting good online safety practice when using digital in and out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school.

Parents/Carers:

Parents/carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website/VLE and information about national/local online safety campaigns/literature. Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- Digital and video images taken at school events.
- Access to parents' sections of the website/VLE and on-line student records.
- Their children's personal devices in the school (where this is allowed)

Policy Statements

Education – Students

Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students in online safety is therefore an essential part of the school's online provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned online safety curriculum is provided through PSE DCF Citizenship and ICT lessons and should be regularly revisited.
- Key online safety messages are reinforced as part of a planned programme of assemblies and tutorial/pastoral activities.
- Students should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Students should be helped to understand the need for the student Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school
- Staff should act as good role models in their use of digital technologies the internet and mobile devices

- In lessons where internet use is pre-planned, it is best practice that students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where students are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs, and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the IT Manager (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need and sent to the help desk.

Education – Parents/Carers:

Parents/carers play an essential role in the education of their children and in the monitoring/regulation of their children's online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and carers through parent sessions, newsletters and Facebook.

Education & Training – Staff/Volunteers:

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety and communications policy and Acceptable Use Agreements.
- The DCF Coordinator/AHT (will receive regular updates through attendance at external training events/other relevant organisations) and by reviewing guidance documents released by relevant organisations.
- This Online Safety policy and its updates will be presented to and discussed by staff in staff/team meetings/INSET days.
- The DCF Coordinator will provide advice, guidance, training to individuals as required.

Training – Governors:

Governors should take part in online safety training and awareness sessions, with particular importance for those who are members of any sub-committee/group involved in technology, online safety, health and safety and child protection. This may be offered in a number of ways:

• Attendance at training provided by the Local Authority/National Governors Association/ or other relevant organisation.
• Participation in school training/information sessions for staff or parents (this may include attendance at assemblies/lessons).

Technical – infrastructure/equipment, filtering and monitoring:

The school will be responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities:

• School technical systems will be managed in ways that ensure that the school meets recommended technical requirements.
• There will be regular reviews and audits of the safety and security of school technical systems
• All users will have clearly defined access rights to school systems and devices.
• All users will be provided with a username and secure password. Users are responsible for the security of their username and password.
• The school has provided enhanced/differentiated user-level filtering
• School technical staff regularly monitor and record the activity of users on the school systems and users are made aware of this in the Acceptable Use Agreement.
• An appropriate system is in place for users to report any actual, potential incident or security breach to the relevant person, as agreed.
• An agreed policy is in place for the provision of temporary access of "guests" (eg trainee teachers, supply teachers, visitors) onto the school systems.
• An agreed policy is in place regarding the extent of personal use that users are allowed on school devices that may be used out of school.
• Users are not permitted to download and or install applications (including executable or similar types) on to a school device or whilst using the schools systems, without agreement from the IT department.
• Users may use the following types of removable media for the purposes detailed:
-CD/DVD – Playing original video material, original music and viewing data written to the media that is owned by the user (who has copyright ownership). The use of software written to writable versions of this media is strictly prohibited.
-USB Media (memory sticks) – this type of media can be used on school devices for transferring personal work, this being data created by the user. The use of applications on this type of media is strictly prohibited.
-Other types of media that may exist may only be used for the movement of personal data where the user owns the copyright.

Bring Your Own Device (BYOD):

The educational opportunities offered by mobile technologies are being expanded as a wide range of devices, software and online services become available for teaching and learning, within and beyond the classroom. This has led to the exploration by schools of users bringing their own technologies in order to provide a greater freedom of choice and usability. However, there are a number of online safety considerations for BYOD. Use of BYOD should not introduce vulnerabilities into existing secure environments. Considerations will need to include; levels of secure access, filtering, data protection, storage and transfer of data, mobile device management systems, training, support, acceptable use, auditing and monitoring.

- The school has a set of clear expectations and responsibilities for all users.
- The school adheres to the Data Protection Act principles.
- All users are provided with and accept the Acceptable Use Agreement. (See BYOD contracts and Appendix 1)
- All network systems are secure and access for users is differentiated.

- Where possible these devices will be covered by the school's normal filtering systems, while being used on the premises.
- All users will use their username and password and keep this safe.
- Students receive training and guidance on the use of personal devices.
- Regular audits and monitoring of usage will take place to ensure compliance.
- Any loss or theft of the device will be reported.

Use of digital and video images:

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and students need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate students about the risks associated with the taking, using, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet eg on social networking sites.
- In accordance with guidance from the Information Commissioner's Office, parents/ carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published or made publicly available on social networking sites, nor should parents/carers comment on any activities involving other students in the digital/video images.
- Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital/video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Students must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images. All photographs that are published must have consent.
- Written permission from parents or carers will be obtained before photographs of students are published on the school website. This information will be collated and stored on SIMS.
- Student's work can only be published with the permission of the student and parents or carers.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 and the schools' Data Protection Policy.
Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.

Communications:

A wide range of rapidly developing communications technologies has the potential to enhance learning. When using communication technologies the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored.
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and students or parents/carers (email, google classroom, Teams, VLE etc) must be professional in tone and content.
- Students should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school/ website and only official email addresses should be used to identify members of staff.
- All staff must comply with the school's Online Safety and Communications Policy.

Social Media - Protecting Professional Identity:

All schools and local authorities have a duty of care to provide a safe learning environment for students and staff. Schools and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place. The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to students, staff and the school through limiting access to personal information:

- Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions.

School staff should ensure that:

- No reference should be made in social media to students, parents/carers or school staff.
- They do not engage in online discussion on personal matters relating to members of the school community.
- Personal opinions should not be attributed to the school or local authority.
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

The school's use of social media for professional purposes will be checked regularly. All use of Social Media should comply with the school's Online Safety and Communications Policy.

Appropriate and Inappropriate Use by Staff or Adults:

Staff members have access to the network so that they can obtain age appropriate resources for their classes and create folders for saving and managing resources. They have a password to access a filtered internet service and know that this should not be disclosed to anyone or leave a computer or other device unattended whilst they are logged in. All staff should receive a copy of the Online Safety and Communications Policy. The school's Acceptable use Agreement (Appendix 1) will appear each time a member of staff logs on, they will need to accept the terms of this agreement in order to use network facilities.
The Acceptable Use Agreement will be displayed in the staff room as a reminder that staff members need to safeguard against potential allegations and a copy of this policy is provided to all staff for home use.
When accessing the Learning Platform from home, the same Acceptable Use Agreement will apply. The acceptable use should be similar for staff to that of the children and young people so that an example of good practice can be established.

In the Event of Inappropriate Use

If a member of staff is believed to misuse the internet or learning platform in an abusive or illegal manner, a report must be made to the Headteacher/AHT immediately and then the Safeguarding and Child Protection Policy or Disciplinary Policy must be followed to deal with any misconduct and all appropriate authorities contacted.

Appropriate and Inappropriate Use by Children or Young People:

Acceptable Use Agreements detail how children and young people are expected to use the internet and other technologies within school, including downloading or printing of any materials. The agreements are there for children and young people to understand what is expected of their behaviour and attitude when using the internet. This will enable them to take responsibility for their own actions. For example, knowing what is polite to write in an e-mail to another child, or understanding what action to take should there be the rare occurrence of sighting unsuitable material. This also includes the deliberate searching for inappropriate materials and the consequences for doing so.
School should encourage parents/carers to support the agreement with their child or young person. This can be shown by signing the Acceptable Use Agreements together so that it is clear to the school setting or other establishment that the agreement are accepted by the child or young person with the support of the parent/carer. This is also intended to provide support and information to parents/carers when children and young people may be using the Internet beyond school setting or other establishment.
Further to this, it is hoped that parents/carers will add to future rule amendments or updates to ensure that they are appropriate to the technologies being used at that time and reflect any potential issues that parents/carers feel should be addressed, as appropriate.
The downloading of materials, for example, music files and photographs need to be appropriate and 'fit for purpose' based on research for work and be copyright free.
File-sharing via e-mail, weblogs or any other means online should be appropriate and be copyright free when using the learning platform in or beyond school/education setting or other establishment.

In the Event of Inappropriate Use

Should a child or young person be found to misuse the online facilities whilst at school, the following consequences should occur:

- If a child is found to be misusing the internet by not following the Acceptable Use Agreement, parents/carers will be contacted to explain the reason for suspending the child or young person's use for a particular lesson or activity.
- Further misuse of the agreement may result in further sanctions which could include not being allowed to access the internet for a period of time.
- A letter may be sent to parents/carers outlining the breach in Safeguarding Policy where a child or young person is deemed to have misused technology against another child or adult.
- In the event that a child or young person accidentally accesses inappropriate materials the child should report this to an adult immediately and take appropriate action to hide the screen or close the window, so that an adult can take the appropriate action. Where a child or young person feels unable to disclose abuse, sexual requests or other misuses against them to an adult, they should report this to an adult.
- The issue of a child or young person deliberately misusing online technologies should also be addressed by the establishment.
- Children should be taught and encouraged to consider the implications for misusing the internet and posting inappropriate materials to websites, for example, as this may have legal implications. This will be done through the DCF Citizenship modules and the BEAT program.

Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff/volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below).

  Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
- Internal response or discipline procedures.
- Involvement by Local Authority or national/local organisation (as relevant).
- Police involvement and/or action.

If content being reviewed includes images of child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the Police would include:

- Incidents of 'grooming' behaviour.
- The sending of obscene materials to a child.
- Adult material which potentially breaches the Obscene Publications Act.

- Criminally racist material.
- Other criminal conduct, activity or materials.
- Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the group for evidence and reference purposes.

Safe and Responsible use of:

(Appendix 2)

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.

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 on page 18.
- 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.

Online Social Communications 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.

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.

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. (Page 18)
- 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.

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.

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.

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.

Staff expectations of the school

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

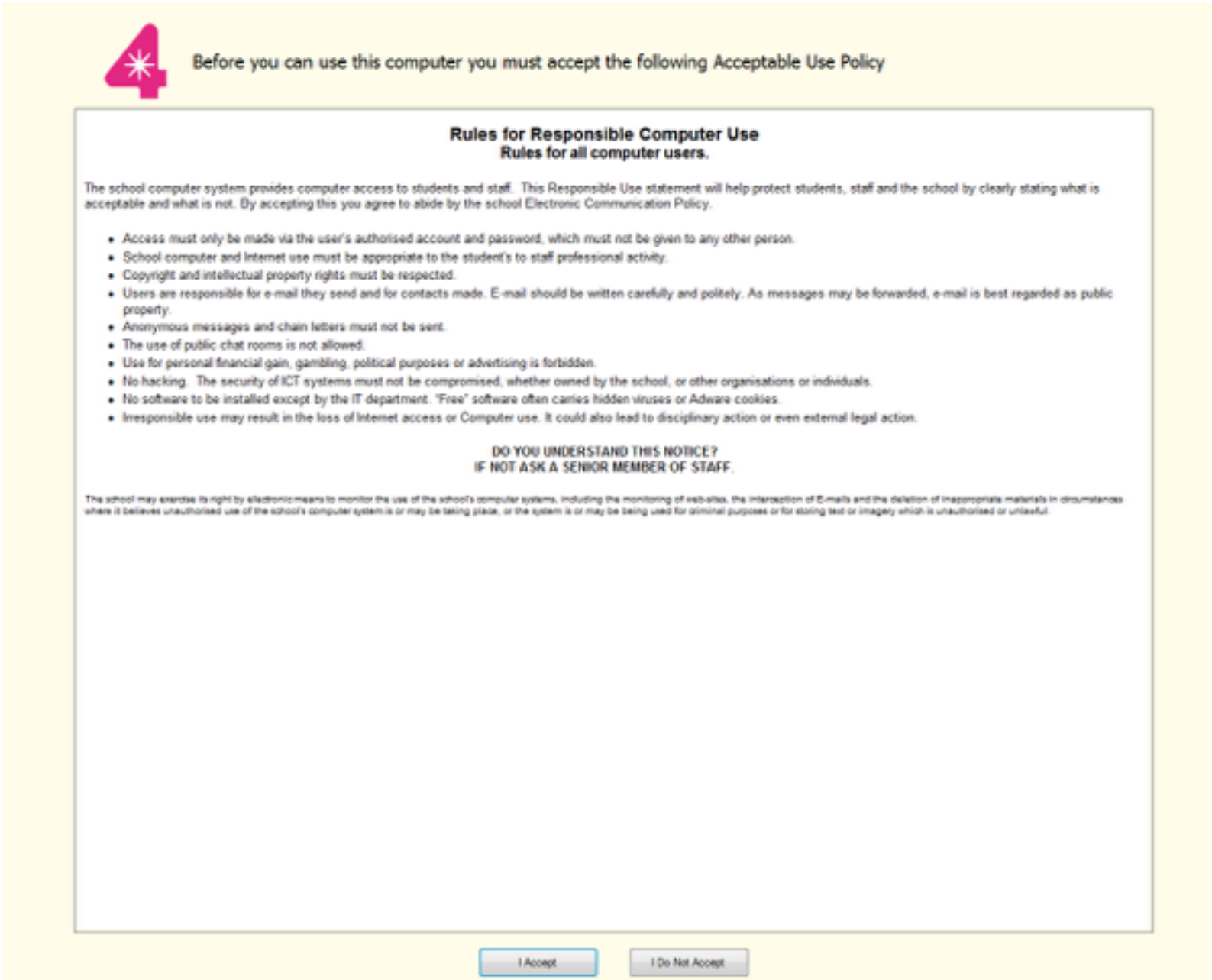
- Enforce policies to protect staff and pupils from malicious use of mobile phones, in particular the use of camera and video functions on phones

- 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.

APPENDIX 1

APPENDIX 2

Secure transfer of data and access out of school



- QEHS recognises that personal data may be accessed by users out of school, or transferred to the LA or other agencies. In these circumstances:
- Users may not remove or copy sensitive or restricted or protected personal data from the school or authorised premises without permission and unless the media is encrypted and password protected and is transported securely for storage in a secure location
- Users must take particular care that computers or removable devices which contain personal data must not be accessed by other users (e.g. family members) when out of school
- When restricted or protected personal data is required by an authorised user from outside the organisation's premises (for example, by a member of staff to work from their home), they should preferably have secure remote access to the management information system or learning platform
- If secure remote access is not possible, users must only remove or copy personal or sensitive data from the organisation or authorised premises if the

storage media, portable or mobile device is encrypted and is transported securely for storage in a secure location

- Users must protect all portable and mobile devices, including media, used to store and transmit personal information using approved encryption software; and
- Particular care should be taken if data is taken or transferred to another country, particularly outside Europe.
- The school will only release personal data if the request has appropriate legal backing.