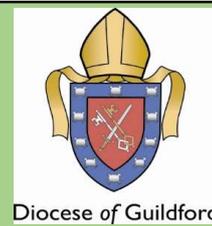


Queen Eleanor's Church of England Junior School  
 An Academy in the Good Shepherd Trust  
 Queen Eleanor's Road, Onslow Village, Guildford, GU2 7SD



## e-SAFETY POLICY

Date	Review Date	Coordinator	Responsible Body
September 2015	March 2017	Whole Staff	Children's Committee

### Introduction

As part of the Every Child Matters agenda set out by the government, the Education Act 2002 and the Children's Act 2004, it is the duty of school to ensure that children and young people are protected from potential harm both within and beyond the school or other establishment environment. Therefore, the involvement of children, young people and parent/carers is also vital to the successful use of online technologies.

### Aims

This policy aims to explain how parents/carers, children or young people can be a part of these safeguarding procedures. It also details how children and young people are educated to be safe and responsible users capable of making good judgements about what they see, find and use. The term 'e-safety' is used to encompass the safe use of all technologies in order to protect children, young people and adults from potential and known risks.

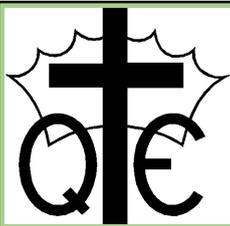
- To emphasise the need to educate staff, children and young people about the pros and cons of using new technologies both within and outside school or other establishment .
- To provide safeguards and agreement for acceptable use to guide all users, whether staff or student, in their online experiences.
- To ensure adults are clear about procedures for misuse of any technologies both within and beyond the school or other establishment.
- To develop links with parents/carers and the wider community ensuring input into policies and procedures with continued awareness of the benefits and potential issues related to technologies.
- To ensure the school's Christian values and ethos are central to ensuring children are kept safe online.

### Roles and Responsibilities of the School or Other Establishment

#### Governors/ Headteacher/Children's Committee members

It is the overall responsibility of the Headteacher with the Governors to ensure that there is an overview of e-Safety as part of the wider remit of safeguarding across the school or other establishment with further responsibilities as follows:

- The Headteacher has designated an e-Safety Lead (the Deputy Headteacher) to implement agreed policies, procedures, staff training, curriculum requirements and take responsibility for ensuring e-Safety is addressed in order to establish a safe ICT learning environment. All staff and students are aware of takes this role within the school or other establishment.
- Time and resources should be provided for the e-Safety Lead and staff to be trained and update policies, where appropriate. This time will be decided on a needs basis.
- The Headteacher is responsible for promoting e-Safety across the curriculum and has an awareness of how this is being developed, linked with the school or other establishment development plan.
- The Headteacher should inform the Governors at the Children's Committee meetings about the progress of or any updates to the e-Safety curriculum (via PSHE or ICT) and ensure Governors know how this relates to safeguarding. At the Full Governor meetings, all Governors are to be made aware of e-Safety developments from the Children's Committee meetings.



## e-SAFETY POLICY

- The Governors **MUST** ensure e-safety is covered within an awareness of safeguarding and how it is being addressed within the school or other establishment. It is the responsibility of Governors to ensure that all safeguarding guidance and practices are embedded.
- An e-Safety Governor (ICT Governor) ought to challenge the school or other establishment about having an Acceptable Use Policy (AUP) with appropriate strategies which define the roles, responsibilities for the management, implementation and safety for using ICT, including:

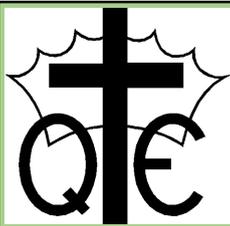
Challenging the school or other establishment about having:

- Firewalls.
  - Anti-virus and anti-spyware software.
  - Filters.
  - Using an accredited ISP (Internet Service Provider).
  - Awareness of wireless technology issues.
  - A clear policy on using personal devices.
- Ensure that any misuse or incident has been dealt with appropriately, according to policy and procedures, (see the Managing Allegations Procedure on Surrey Local Safeguarding Children's Board website) and appropriate action is taken, even to the extreme of suspending a member of staff, informing the police (via establishment's agreed protocols with the police) or involving parents/carers.

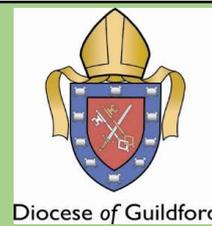
### Local e-Safety Lead

It is the role of the designated e-Safety Lead to:

- Appreciate the importance of e-safety within school or other establishment and to recognise that all educational establishments have a general duty of care to ensure the safety of their pupils and staff.
- Establish and maintain a safe ICT learning environment within the school or other establishment.
- Ensure that the AUP is reviewed annually, with up-to-date information and that training is available for all staff to teach e-Safety and for parents to feel informed and know where to go for advice.
- Ensure that filtering is set to the correct level for staff, children and young people, in the initial set up of a network, stand-a-lone PC, staff/children laptops and the learning platform
- Ensure that all adults are aware of the filtering levels and why they are there to protect children and young people.
- Report issues and update the Headteacher on a regular basis.
- Liaise with the PSHE, safeguarding and ICT leads so that policies and procedures are up-to-date to take account of any emerging issues and technologies.
- Update staff training (all staff) according to new and emerging technologies so that the correct e-safety information can be taught or adhered to.
- Transparent monitoring of the Internet and online technologies
- Keep a log of incidents for analysis to help inform future development and safeguarding, where risks can be identified. Refer to the Managing Allegations Procedure from the SSCB to ensure the correct procedures are used with incidents of misuse.
- Work alongside the ICT Subject Leader, to ensure there is appropriate and up-to-date anti-virus software and anti-spyware on the network, stand-a-lone PCs and teacher/child laptops and that this is reviewed and updated on a regular basis.



Queen Eleanor's Church of England Junior School  
*An Academy in the Good Shepherd Trust*  
Queen Eleanor's Road, Onslow Village, Guildford, GU2 7SD



Diocese of Guildford

## e-SAFETY POLICY

- Ensure that staff can check for viruses on laptops, stand-a-lone PCs and memory sticks or other transferable data files to minimise issues of virus transfer.
- Ensure that unsolicited e-mails to a member of staff from other sources is minimised through the use of e-mail filtering
- Refer to the Managing Allegations Procedure, SSCB, for dealing with any issues arising from indecent or pornographic/child abuse images sent/received.
- Ensure there is regular monitoring of internal e-mails, where:
  - Blanket e-mails are discouraged
  - Tone of e-mails is in keeping with all other methods of communication
- Report overuse of blanket e-mails or inappropriate tones to the Headteacher and/or Governors.

The e-Safety Lead for Queen Eleanor's is Mr Paul Day who has undergone the CEOP training.

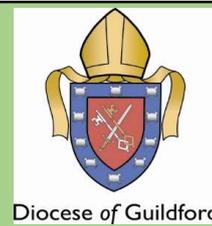
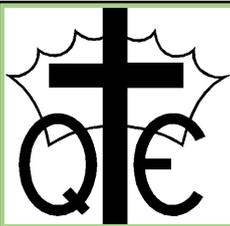
### Staff or Adults

It is the responsibility of all adults within the school or other establishment to:

- Ensure that they know who the Senior Designated Person for Safeguarding is (Child Protection Liaison Officer - CPLO) within school or other establishment, so that any misuse or incidents can be reported which involve a child.
- Where an allegation is made against a member of staff it should be reported immediately to the Headteacher or CPLO.

### **In the event of an allegation made against the Headteacher, the Chair of Governors must be informed immediately**

- Be familiar with the Behaviour, Anti-bullying and other relevant policies so that, in the event of misuse or an allegation, the correct procedures can be followed immediately. In the event that a procedure is unknown, they will refer to the Headteacher or CPLO immediately, who should then follow the Managing Allegations Procedure, where appropriate.
- Check the filtering levels are appropriate for their children and young people and are set at the correct level. Report any concerns to the e-Safety Lead.
- Alert the e-Safety Lead of any new or arising issues and risks that may need to be included within policies and procedures.
- Ensure that children and young people are protected and supported in their use of technologies so that they know how to use them in a safe and responsible manner. Children and young people should know what to do in the event of an incident.
- Be up-to-date with e-Safety knowledge that is appropriate for the age group and reinforce through the curriculum.
- Sign an Acceptable Use Statement to show that they agree with and accept the agreement for staff using non-personal equipment, within and beyond the school or other establishment environment, as outlined in appendices.



## e-SAFETY POLICY

- Use electronic communications in an appropriate way that does not breach the Data Protection Act 1998. Remember confidentiality and not disclose information from the network, pass on security passwords or leave a station unattended when they or another user is logged in.
- To ensure that School or other establishment bursars follow the correct procedures for any data required to be taken from the school or other establishment premises.
- Report accidental access to inappropriate materials to the e-Safety Lead and school or other establishment helpdesk in order that inappropriate sites are added to the restricted list or control this with the Local Control options via your broadband connection.
- Use anti-virus software and check for viruses on their work laptop, memory stick or a CD ROM when transferring information from the internet on a regular basis, especially when not connected to the school or other establishment's network.
- Ensure that all personal storage devices (i.e. memory sticks) which are utilised by staff members to hold sensitive information are encrypted or password protected in the event of loss or theft.
- Report incidents of personally directed "bullying" or other inappropriate behaviour via the Internet or other technologies using the SCC accident/incident reporting procedure in the same way as for other non-physical assaults.

### Children and Young People

Children and young people should be:

- Involved in the review of Acceptable Use Agreement through the school or other establishment council or other appropriate group, in line with this policy being reviewed and updated.
- Responsible for following the Acceptable Use Agreement whilst within school or other establishment as agreed at the beginning of each academic year or whenever a new child attends the school or other establishment for the first time.
- Taught to use the internet in a safe and responsible manner through ICT, PSHE or other clubs and groups.
- Taught to tell an adult about any inappropriate materials or contact from someone they do not know straight away, without reprimand (age and activity dependent).

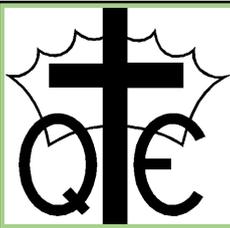
### Appropriate and Inappropriate Use by Staff or Adults

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 Acceptable Use Policy and a copy of the Acceptable Use Agreement, which they need to sign, return to the school or other establishment, to keep under file with a signed copy returned to the member of staff.

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.



Queen Eleanor's Church of England Junior School  
*An Academy in the Good Shepherd Trust*  
Queen Eleanor's Road, Onslow Village, Guildford, GU2 7SD



Diocese of Guildford

## e-SAFETY POLICY

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 or CPLO immediately and then the Managing Allegations Procedure and the Child Protection Policy must be followed to deal with any misconduct and all appropriate authorities contacted.

In the lesser event of misuse or accidental misuse refer to appendices for a list of actions relating to the scale of misuse.

### **By Children or Young People**

Acceptable Use Agreements and the letter for children, young people and parents/carers are outlined in the Appendices. These detail how children and young people are expected to use the internet and other technologies within school or other establishment, 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.

The 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 or other establishment that the agreement are accepted by the child or young person with the support of the parent/carers. This is also intended to provide support and information to parents/carers when children and young people may be using the Internet beyond school 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.

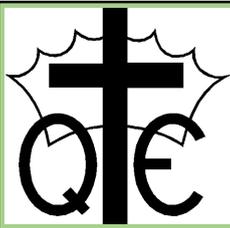
The downloading of materials, for example, music files and photographs need to be appropriate and 'fit for purpose' based on research for work and be copyright free.

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 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 or other establishment, the following consequences should occur:

- Any child found to be misusing the internet by not following the Acceptable Use Agreement may have a letter sent home to parents/carers explaining 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 not being allowed to access the internet for a period of time and another letter will be sent home to parents/carers.



Queen Eleanor's Church of England Junior School  
An Academy in the Good Shepherd Trust  
Queen Eleanor's Road, Onslow Village, Guildford, GU2 7SD



Diocese of Guildford

## e-SAFETY POLICY

- 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, e.g. use 'Hector Protector', for example, (dependent on age) 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 can use the Report Abuse button ([www.thinkuknow.co.uk](http://www.thinkuknow.co.uk)) to make a report and seek further advice. 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.

### The Curriculum and Tools for Learning

#### Internet Use

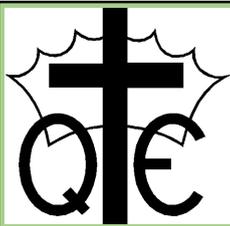
School should teach children and young people how to use the Internet safely and responsibly. They should also be taught, through ICT and/or PSHE lessons, how to research information, explore concepts and communicate effectively in order to further learning. The following concepts, skills and competencies should have been taught by the time they leave *Year 6*:

- Internet literacy.
- Making good judgements about websites and e-mails received.
- Knowledge of risks such as viruses and opening mail from a stranger.
- Access to resources that outline how to be safe and responsible when using any online technologies.
- Knowledge of copyright and plagiarism issues.
- File sharing and downloading illegal content.
- Uploading information – know what is safe to upload and not upload personal information.
- Where to go for advice and how to report abuse.

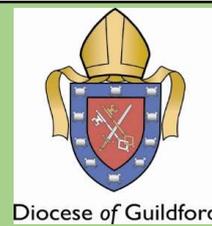
These skills and competencies are taught within the curriculum so that children and young people have the security to explore how online technologies can be used effectively, but in a safe and responsible manner. Children and young people should know how to deal with any incidents with confidence, as we adopt the 'never blame the child for accidentally accessing inappropriate materials' culture, in the event that they have **accidentally** accessed something.

Personal safety – ensuring information uploaded to web sites and e-mailed to other people does not include any personal information such as:

- Full name (first name is acceptable, without a photograph).
- Address.
- Telephone number.
- E-mail address.
- School or other establishment.
- Clubs attended and where.
- Age or DOB.
- Names of parents.
- Routes to and from school or other establishment.
- Identifying information, e.g. I am number 8 in the school or other establishment Football Team.



Queen Eleanor's Church of England Junior School  
*An Academy in the Good Shepherd Trust*  
Queen Eleanor's Road, Onslow Village, Guildford, GU2 7SD



Diocese of Guildford

## e-SAFETY POLICY

Photographs should only be uploaded on the approval of a member of staff or parent/carer and should only contain something that would also be acceptable in 'real life'. Parents/carers should monitor the content of photographs uploaded. Images of children and young people should be stored according to policy.

### **Pupils with Additional Learning Needs**

The school or other establishment should strive to provide access to a broad and balanced curriculum for all learners and recognise the importance of tailoring activities to suit the educational needs of each pupil. Where a student has specific learning requirements, or poor social understanding, careful consideration is given to the planning and delivery of e-safety awareness sessions and internet access.

### **Learning Platforms**

Surrey's learning platform provides a wealth of opportunity for adults, children and young people within and beyond school or other establishment to:

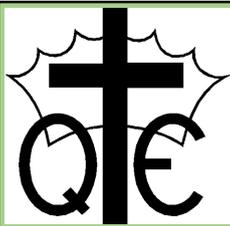
- Access resources via the National Education Network (NEN), which extends regionally to support school.
- Collaborate and share work via web cams and uploading.
- Ask questions.
- Debate issues.
- Dialogue with peers.
- Dialogue with family members or carers.
- Access resources in real time.
- Access other people and cultures in real time.
- Develop an online community.

The tools available for use within the learning platform for adults, children and young people include:

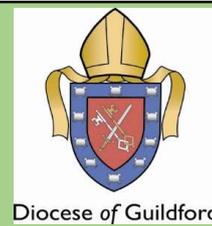
- Internet access.
- E-mail.
- Video-conferencing.
- Weblogs (online diaries).
- Wikis (online encyclopaedia or dictionary).
- Instant Messaging.
- An online personal space for adapting as a user to:
  - Upload work.
  - Access calendars and diaries.
  - Blog.

The personal space contained on a learning platform is designed to provide young users with the facility to share information and work collaboratively with others members of Surrey's enable community. It should be noted that learning platforms provide the user with a private area where they may store information about themselves, accessible only to other platform users via an 'invite' system. Before students access and populate this area, guidance and support should be given to young people regarding the appropriate use of personal details on social networking sites (such as Facebook and Bebo) and how to keep themselves safe whilst online.

Children and young people should use their login and password to access the internet via the learning platform so that the level of filtering is appropriate. Staff should be ensuring that children and young people are not bypassing the login to get to the learning platform so that they are protected to the best of the school or other establishment's ability, in line with E2BN, AUP and SCC policy.



Queen Eleanor's Church of England Junior School  
*An Academy in the Good Shepherd Trust*  
Queen Eleanor's Road, Onslow Village, Guildford, GU2 7SD



Diocese of Guildford

## e-SAFETY POLICY

Staff or adults need to ensure they consider the risks and consequences of anything they or their children and young people may post to any web or social networking sites, as inappropriate comments or images can reflect poorly on an individual and can affect future careers.

### **School or Other Establishment Website (If Different To the Learning Platform Space)**

The uploading of images to the school or other establishment website should be subject to the same acceptable agreement as uploading to any personal online space. Permission ought to be sought from the parent/carer prior to the uploading of any images. Settings should consider which information is relevant to share with the general public on a website and use secure areas for information pertaining to specific audiences.

### **External Websites**

In the event that a member of staff finds themselves or another adult on an external website, such as 'Rate My Teacher', as a victim, school are encouraged to report incidents to the Headteacher and unions, using the reporting procedures for monitoring.

### **E-mail Use**

The school or other establishment should have E-mail addresses for children and young people to use, as a class and/or as individuals as part of their entitlement to being able to understand different ways of communicating and using ICT to share and present information in different forms.

Individual email accounts can be traced if there is an incident of misuse whereas class email accounts cannot, especially for older users.

Staff, children and young people should use their school or other establishment issued email addresses for any communication between home and school or other establishment only. A breach of this may be considered a misuse.

Parents/carers are encouraged to be involved with the monitoring of emails sent, although the best approach with children and young people is to communicate about who they may be talking to and assess risks together.

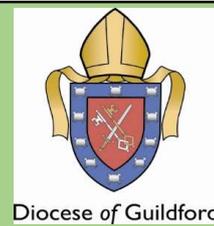
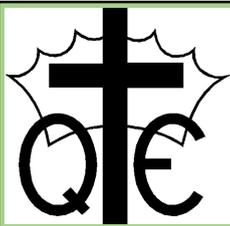
Teachers are expected to monitor their class use of emails where there are communications between home and school or other establishment/setting, on a regular (weekly or as necessary) basis. Where an establishment has a network manager, there is an expectation that monitoring software is used to flag up inappropriate terms and that a senior member of the team has an overview of potential issues on a regular basis – refer to the Monitoring section for further information.

### **Mobile Phones and Other Emerging Technologies**

The school carefully considers how the use of mobile technologies can be used as a teaching and learning tool within the curriculum with the following areas of concern to be taken into consideration:

- Inappropriate or bullying text messages.
- Images or video taken of adults or peers without permission being sought.
- Wireless Internet access, which can bypass school or other establishment filtering and allow access to inappropriate or potentially harmful material or communications.

It is important to consider that increased incidents of bullying and misuse have been reported where students are allowed to use them in school or other establishment. In settings where clear agreement on this issue are agreed to and followed, the level of misuse is reduced. Where inappropriate usage of said technologies does occur a virtual paper trail may be traceable, even if the message received is sent anonymously.



## e-SAFETY POLICY

### (i) Personal Mobile Devices

Staff should be allowed to bring in personal mobile phones or devices for their own use, but **must not use personal numbers to contact children and young people under any circumstances.**

- Staff must ensure that there is no inappropriate or illegal content stored on the device and should be aware that using features, such as video or sound recording, may be subject to the same procedures as taking images from digital or video cameras (see below for further details).
- Staff should be aware that games consoles such as the Sony play station, Microsoft Xbox, Nintendo Wii and DSi and other such systems have Internet access which may not include filtering. Before use within school or other establishment, authorisation should be sought from the Headteacher and the activity supervised by a member of staff at all times.
- The school or other establishment is not responsible for any theft, loss or damage of any personal mobile device.

### (ii) School or Other Establishment Issued Mobile Devices

The management of the use of these devices should be similar to those stated above, but with the following additions:

- Where the establishment has provided a mobile device to a member of staff, such as a laptop, PDA or mobile phone, only this equipment should be used to conduct school or other establishment business outside of the school or other establishment environment.

It should also be policy to ensure that children and young people understand the use of a public domain and the consequences of misuse. Relevant curriculum links should be made to highlight the legal implications and the involvement of law enforcement. Other technologies which school/education settings and other establishments use with children and young people include:

- . Photocopiers.
- . Fax machines.
- . Telephones.

### Video and Photographs

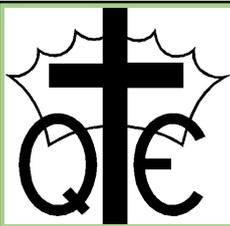
The term 'image' refers to the taking of video footage or photographs via any camera or other technology, e.g. a mobile phone.

When in school or establishment there is access to PCs and Netbooks with webcams

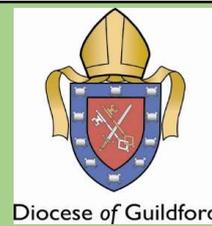
It is also highly recommended that permission is sought prior to any uploading of images to check for inappropriate content.

The sharing of photographs via weblogs, forums or any other means online should only occur after permission has been given by a parent/carer or member of staff.

Photographs/images used to identify children and young people in a forum or using Instant Messaging within the learning platform should be representative of the child rather than of the child e.g. an avatar.



Queen Eleanor's Church of England Junior School  
An Academy in the Good Shepherd Trust  
Queen Eleanor's Road, Onslow Village, Guildford, GU2 7SD



Diocese of Guildford

## e-SAFETY POLICY

Any photographs or video clips uploaded should not have a file name of a child, especially where these may be uploaded to a school or other establishment website. Photographs should only ever include the child's first name although safeguarding guidance states either a child's name or a photograph but not both.

Group photographs are preferable to individual children and young people and should not be of any compromising positions or in inappropriate clothing, e.g. gym kit. The School or other establishment will need to decide how photographs will be used, including where they will be stored (central location which could be viewed by anyone) and when they will be deleted.

It is current practice by external media such as local and national newspapers to include the full name of children and young people in their publications. Photographs of children/young people should only be used after permission has been given by a parent/carer.

### Webcams

Taking images via a webcam should follow the same procedures as taking images with a digital or video camera.

Children need to tell an adult immediately of any inappropriate use by another child or adult. (This is part of the Acceptable Use Agreement).

Where children, young people (or adults) may be using a webcam in a family area at home, they should have open communications with parents/carers about their use and adhere to the Acceptable Use Agreement.

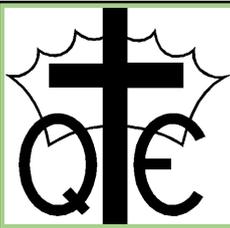
### Social Networking Advice for Staff

Social networking outside of work hours, on non-school or other establishment-issue equipment, is the personal choice of all school or other establishment staff. Owing to the public nature of such websites, it is advisable for staff to consider the possible implications of participation. The following advice should be considered if involved in social networking:

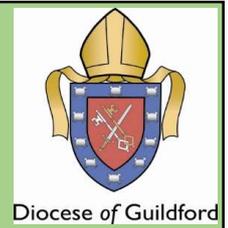
- Personal details are never shared with pupils such as private email address, telephone number or home address. It is recommended that staff ensure that all possible privacy settings are activated to prevent students from making contact on personal profiles. The simplest and most effective way to do this is to remove details from search results and turn off public visibility.
- Staff should not engage in personal online contact with students outside of Headteacher authorised systems (e.g. school or other establishment email account for homework purposes).
- Staff should ensure that full privacy settings are in place to prevent students from accessing photo albums or personal information.
- Staff are advised against accepting invites from colleagues until they have checked with them in person that the invite is genuine (avoiding fake profiles set up by students).
- There is well documented evidence to suggest that social networking can be a highly effective tool for communicating with students on a **professional** level. Some school, other educational and other settings have set up accounts on Facebook to manage and monitor public and pupil communications through designated members of staff. Other such professional social networking tools include Edmodo or Virtual Learning Environments such as Moodle which contain similar features.

### Safeguarding Measures – Filtering

Staff, children and young people are required to use the personalised learning space and all tools within it, in an acceptable way.



Queen Eleanor's Church of England Junior School  
An Academy in the Good Shepherd Trust  
Queen Eleanor's Road, Onslow Village, Guildford, GU2 7SD



## e-SAFETY POLICY

Please refer to the Acceptable Use Agreement for Staff and children and young people for the appropriate use of the learning platform.

The RM broadband connectivity has a filter system which should be set at an age appropriate level so that inappropriate content is filtered and tools are appropriate to the age of the child. **All** filtering should be set to 'No Access' within any setting and then controlled via:

- Portal Control (controls filtering at local site level) which controls individual access to the Internet.
- Local Control – controls access to websites and provides the option to add to a 'restricted list'.

Anti-virus and anti-spyware software is used on all network and stand-alone PCs or laptops and is updated on a regular basis.

A firewall ensures information about children and young people and the school cannot be accessed by unauthorised users.

Children should use a search engine that is age appropriate such as AskJeeveskids or Yahoo!igans.

CEOP (Child Exploitation and Online Protection Centre) training for children is annual and part of the PSHE curriculum for raising awareness on staying safe and being responsible. A link to the [www.thinkukknow.co.uk](http://www.thinkukknow.co.uk) website is part of the skin layout for further advice and information on children or young people's personal online spaces.

### Monitoring

The e-Safety Lead and/or a senior member of staff should be monitoring the use of online technologies by children and young people and staff, on a regular basis.

Teachers should monitor the use of the learning platform and Internet during lessons and also monitor the use of e-mails from school or other establishment and at home, on a regular basis.

### School or Other Establishment Library

The computers in the school or other establishment library should be protected in line with the school or other establishment network.

Where software is used that requires a child login, this ought to be password protected so that the child is only able to access themselves as a user. Children and young people should be taught not to share passwords.

The same acceptable use agreement applies for any staff and children and young people using this technology.

### Parents – Roles

Each child or young person should receive a copy of the Acceptable Use Agreement on an annual basis or first-time entry to the school or other establishment which needs to be read with the parent/carer, signed and returned to school or other establishment, confirming both an understanding and acceptance of the agreement.

It should be expected that parents/carers will explain and discuss the agreement with their child, where appropriate, so that they are clearly understood and accepted.

School or other establishment should keep a record of the signed forms.

### Resources



Queen Eleanor's Church of England Junior School  
An Academy in the Good Shepherd Trust  
Queen Eleanor's Road, Onslow Village, Guildford, GU2 7SD



Diocese of Guildford

## e-SAFETY POLICY

The school or other establishment:

- Can use the Childnet International 'KnowITAll for Parents' CD/online materials (<http://www.childnet-int.org.uk/kia/parents/cd/>) to deliver key messages and raise awareness for parents/carers and the community.
- Ensure that skills around internet use are offered as part of the follow-up training for parents/carers so they know how to use the tools their children and young people are using.
- Endeavour to provide access to the internet for parents/carers so that appropriate advice and information can be accessed where there may be no internet at home, subject to arrangement.

The Appendices detail where parents/carers can go for further support beyond the school or other establishment.

### Links to Other Policies - Behaviour and Anti-Bullying Policies

Please refer to the Behaviour Policy for the procedures in dealing with any potential bullying incidents via any online communication, such as mobile phones, e-mail or blogs. School should have an up to date Anti-bullying Policy, which will include any cyber bullying issues.

All behaviours should be seen and dealt with in exactly the same way, whether on or off-line and this needs to be a key message which sits within all ICT and PSHE materials for children and young people and their parents/carers. People should not treat online behaviours differently to off-line behaviours and should have exactly the same expectations for appropriate behaviour. This is a key message which should be reflected within Behaviour and Anti-bullying Policies as it is only the tools and technologies that change, not the behaviour of children, young people and adults.

### Managing Allegations against Adults Who Work With Children and Young People

Please refer to the Managing Allegation Procedure, in order to deal with any incidents that occur as a result of using personal mobile or e-mail technologies. The procedures detail how to deal with allegation of misuse or misconduct being made by any member of staff or child about a member of staff.

Allegations made against a member of staff should be reported to the Senior Designated Person (SDP) for safeguarding within the school or other establishment immediately. In the event of an allegation being made against a Head teacher, the Chair of Governors should be notified immediately.

### Local Authority Designated Officer (LADO) - Managing Allegations:

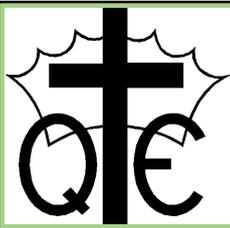
The Local Authority has designated Officers who are involved in the management and oversight of individual cases where there are allegations against an adult in a position of trust. They provide advice and guidance to all of the above agencies and services, and monitor the progress of the case to ensure all matters are dealt with as quickly as possible, consistent with a thorough and fair process. In addition to this they liaise with the police and other agencies.

### Disciplinary Procedure for All School or Other Establishment Based Staff

In the event that a member of staff may be seen to be in breach of behaviour and good conduct through misuse of online technologies, this policy outlines the correct procedures for ensuring staff achieve satisfactory standards of behaviour and comply with the rules of the Governing Body.

### Curriculum Development

The teaching and learning of e-Safety should be embedded within the school/education establishment curriculum to ensure that the key safety messages about engaging with people are the same whether children and young people



Queen Eleanor's Church of England Junior School  
*An Academy in the Good Shepherd Trust*  
Queen Eleanor's Road, Onslow Village, Guildford, GU2 7SD



Diocese of Guildford

## e-SAFETY POLICY

are on or off line. This may form part of the PHSE module but is not exclusive to this area of curriculum and opportunities to embed e-Safety throughout the curriculum should be sought.

### **Health and Safety**

Refer to the Health and Safety Policy and procedures of the school or other establishment and the County Council for information on related topics, particularly Display Screen Equipment, Home working and Accident/Incident reporting procedures. Wireless technologies are not considered to be a hazard following advice from the Health Protection Agency to the Government.

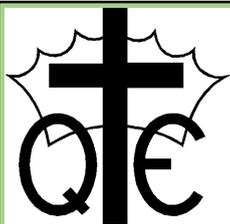
### **CCTV (where applicable)**

To comply with both the Data Protection Act 1998 and the Information Commissioner's CCTV Code of Practice, all school using CCTV for security and safety purposes must publicly declare that they are doing so. The school or other establishment should have erected a sign to inform members of the public that they are entering a surveillance area and to display the following key information.

- The name of the school or other establishment/individuals responsible for the CCTV system.
- The contact details of who is responsible for the system.
- The purpose of the CCTV system.

The school or other establishment must ensure that all images recorded through the CCTV system are fully traceable with the date, time, recording device and person responsible for recording all detail in a secure log for audit trail purposes.

A robust and thoughtful collection of Standard Operating Procedures should be in place to govern the day to day operation of the CCTV system. For data security purposes a restricted number of staff should have access to any images and recordings held by the school or other establishment.



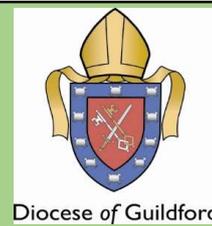
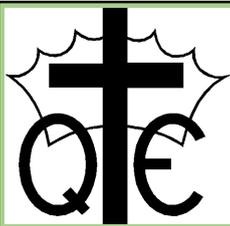
Queen Eleanor's Church of England Junior School  
*An Academy in the Good Shepherd Trust*  
Queen Eleanor's Road, Onslow Village, Guildford, GU2 7SD



Diocese of Guildford

## e-SAFETY POLICY

<b>Headteacher:</b>		<b>Date:</b>	September 2016
<b>Chair of Governors:</b>		<b>Date:</b>	September 2016
<b>Policy Number:</b>			



Appendix 1.

## Acceptable Use Agreement for Staff, Governors and Visitors

### School Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of ICT in their everyday work.

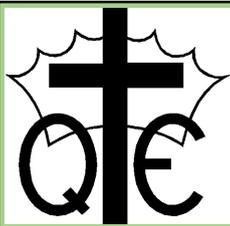
The school will try to ensure that staff and volunteers will have good access to ICT to enhance their work, to enhance learning opportunities for students / pupils learning and will, in return, expect staff and volunteers to agree to be responsible users.

### Acceptable Use Policy Agreement

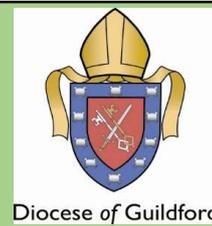
I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that students / pupils receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed e-safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of school ICT systems (e.g. laptops, email, VLE etc.) out of school.
- I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password.



Queen Eleanor's Church of England Junior School  
*An Academy in the Good Shepherd Trust*  
Queen Eleanor's Road, Onslow Village, Guildford, GU2 7SD



Diocese of Guildford

## e-SAFETY POLICY

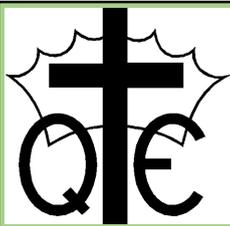
- I will immediately report any illegal, inappropriate or harmful material or incident I become aware of, to the appropriate person.

I will be professional in my communications and actions when using school ICT systems:

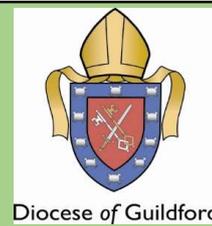
- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (eg on the school website / VLE) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use chat and social networking sites in school in accordance with the school's policies.
- I will only communicate with students / pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner. I understand it is inappropriate for me to use a personal e-mail for school business.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my personal hand held / external devices (PDAs / laptops / mobile phones / USB devices etc.) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not use personal email addresses on the school ICT systems unless absolutely necessary.
- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
- I will ensure that my data is regularly backed up.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.



Queen Eleanor's Church of England Junior School  
An Academy in the Good Shepherd Trust  
Queen Eleanor's Road, Onslow Village, Guildford, GU2 7SD



## e-SAFETY POLICY

- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School / LA Personal Data Policy. Where personal data is transferred outside the secure school network, it must be encrypted.
- I understand that data protection policy requires that any staff or student / pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- When using the internet in my professional capacity or for school sanctioned personal use:
- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of school:

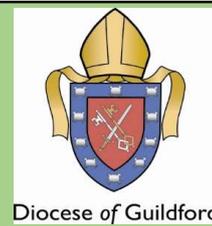
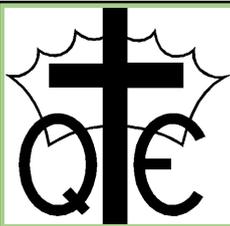
I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment out of school and my use of personal equipment in school or in situations related to my employment by the school.

I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and / or the Local Authority and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff / Volunteer Name

Signed



## e-SAFETY POLICY

### Appendix 2. Acceptable Use Policy for Young People (Below Academic Year 10)

#### My e-Safety Agreement

This is my agreement for using the internet safely and responsibly.

### Acceptable Use Policy for Young People

- I will use the internet to help me learn.
- I will learn how to use the internet safely and responsibly.
- I will only send email messages that are polite and friendly.
- I will only email, chat to or video-conference people I know in the real world or that a trusted adult has approved.
- Adults are aware when I use online tools such as video conferencing.
- I agree never to give out passwords or personal information like my full name, address or phone numbers.
- I agree never to post photographs or video clips without permission or that I will not include my full name with photographs.
- If I need help I know who I can ask and that I can go to [www.thinkuknow.co.uk](http://www.thinkuknow.co.uk) for help if I cannot talk to a trusted adult.
- If I see anything on the internet that makes me feel uncomfortable, I know what to do.
- If I receive a message sent by someone I don't know, I know what to do.
- I know I should follow these guidelines as part of the agreement with my parent/carer.
- I agree to look after myself and others by using my internet in a safe and responsible way.

Signed..... Dated.....

Name.....(Printed)