Manners Makyth Man

NATIONAL
CHURCH OF ENGLAND
ACADEMY

E-Safety Policy

Process:

Policy / Policy Update Presented by/on behalf of:	Associate Principal	28th April 2016
Presented to:	Behaviour, Safety & Ethos Portfolio Team	Agreed 28th April 2016
Approved/Ratified:	Academy Board	**Approved/Ratified** **16th June 2016**

Date of policy/latest review:	Sept 18 – Removal of photo permissions section.
Next review:	Sept 19

What is an E-safety Policy?

- The Academy’s e-safety policy aims to create an environment where pupils, staff, parents, governors and the wider academy community work together to inform each other of ways to use the internet responsibly, safely and positively.

- Internet technology helps pupils learn creatively and effectively and encourages collaborative learning and the sharing of good practice amongst all the academy’s stakeholders. The e-safety policy encourages appropriate and safe conduct and behaviour when achieving this.

- Pupils, staff and all other users of academy related technologies will work together to agree standards and expectations relating to usage in order to promote and ensure good behaviour.

- These agreements and their implementation will promote positive behaviour which can transfer directly into each pupil’s adult life and prepare them for experiences and expectations in their future life. The policy is not designed to be a blacklist of prohibited activities, but instead a list of areas to discuss, teach and inform, in order to develop positive behaviour and knowledge leading to a safer internet usage and year on year improvement and measurable impact on e-safety. It is intended that the positive effects of the policy will be seen online and offline; in academy and at home; and ultimately beyond academy and into the workplace.

Academy Name: National Church of England Academy

Date: May 2014

Contents:

Introduction

Ofsted statements:

Ofsted have defined e-safety thus:

- ‘In the context of an inspection, e-safety may be described as the academy’s ability to protect and educate pupils and staff in their use of technology and to have the appropriate mechanisms to intervene and support any incident where appropriate.’

E-safety will be inspected in relation to the following areas:

- The behaviour and safety of pupils at the academy.
- The quality of leadership in, and management of, the academy

Ofsted have identified three areas of e-safety risk in relation to pupils:

- Being exposed to illegal, inappropriate or harmful material.
- Being subjected to harmful online interaction with other users.
- Personal online behaviour that increases the likelihood of, or causes, harm.

An outstanding academy will demonstrate that:

- “All groups of pupils feel safe at the academy and at alternative provision placements at all times. They understand very clearly what constitutes unsafe situations and are highly aware of how to keep themselves and others safe, including in relation to e-safety.”

E-safety Policy Scope

- The academy’s e-safety Policy and agreements apply to all pupils, staff, support staff, external contractors and members of the wider academy community who use, have access to or maintain the academy and academy related internet and computer systems internally and externally.
- The academy will make reasonable use of relevant legislation and guidelines to affect positive behaviour regarding ICT and internet usage both on and off the academy site. This will include imposing rewards and sanctions for behaviour and penalties for inappropriate behaviour – as defined as regulation of student behaviour under the Education and Inspections Act 2006. ‘In Loco Parentis’ provision under the Children Act 1989 also allows the academy to report and act on instances of cyber bullying, abuse, harassment, malicious communication and grossly offensive material; including reporting to the police, social media websites, and hosting providers on behalf of pupils.

The e-safety policy covers the use of:

- Academy based ICT systems and equipment
- Academy based intranet and networking
- Academy related external internet, including but not exclusively, extranet, e-learning platforms, blogs, social media websites
- External access to internal academy networking, such as webmail, network access, file-serving (document folders) and printing.
- Academy ICT equipment off-site, for example staff laptops, digital cameras, mobile phones.
- Pupil and staff personal ICT equipment when used in academy and which makes use of academy networking, file-serving or internet facilities.
- Mobile phones, devices and laptops when used on the academy site.
- Documents sent to external email accounts.

Reviewing and evaluating e-safety and ensuring good practice

Monitoring the e-safety policy:

The e-safety policy will be actively monitored and evaluated by an e-safety committee. This committee will comprise:

- E-safety Coordinator/Officer
- Principal and Academy Leadership Team.
- Child Protection Officer
- ICT technical support and Network Manager.

Policy review schedule:

- This policy was approved by Behaviour, Safety and Ethos Governor Portfolio commitee and is published for viewing by parents and the wider academy community here: www.nationalce-ac.org.uk
- The e-safety policy will be reviewed annually.
- The e-safety policy will be reviewed and evaluated promptly in the light of serious e-safety incidents.
- The e-safety policy will be reviewed and evaluated promptly in the light of important changes to legislation or government guidance related to e-safety.
- The e-safety committee and e-safety Coordinator/Officer will include in reports evaluations of the impact of the e-safety policy by evidencing – for example - e-safety incidents, contemporaneous written reports, statistics of filtering breaches, logs of internet and network traffic activity, AfL teaching questionnaires and e-safety audits of staff, support staff, parents, governors and other stakeholders, ParentView and Ofsted questionnaire results.

Who does e-safety affect, who is responsible for e-safety and what are their roles?

The academy e-safety Officer or Coordinator:

- The academy has a designated e-safety officer who reports to the SLT and Governors and coordinates e-safety provision across the academy and wider academy community. The e-safety officer liaises with SLT, the academy's designated Child Protection officer and other senior managers as required.
- The academy e-safety coordinator audits and assesses INSET requirements for staff, support staff and governor e-safety training, and ensures that all staff are aware of their responsibilities and the academy's e-safety procedures. The coordinator is also the first port of call for staff requiring advice on e-safety matters.
- Although all staff are responsible for upholding the academy's e-safety policy and safer internet practice, the e-safety Coordinator, and ICT support technician are responsible for monitoring internet usage by pupils and staff, and on academy machines, such as laptops used off-site.
- The e-safety Coordinator is responsible for promoting best practice in e-safety within the wider academy community, including providing and being a source of information for parents and partner stakeholders.

Network manager:

- Internal ICT support staff and technicians are responsible for maintaining the academy's networking, IT infrastructure and hardware. They need to be aware of current thinking and trends in IT security and ensure that the academy system, particularly file-sharing and access to the internet is secure. They need to further ensure that all reasonable steps have been taken to ensure that systems are not open to abuse or unauthorised external access, with particular regard to external logins and wireless networking.
- ICT Support staff also need to monitor and maintain internet filtering.
- The network manager will also liaise with external organisations such as social media sites regarding e-safety issues if they arise.

Child Protection Officer:

- The academy e-safety coordinator maintains a log of submitted e-safety reports and incidents.
- The Child Protection Officer needs to be able to differentiate which e-safety incidents are required to be reported to CEOP, local Police, LADO, social services and parents/guardians; and also determine whether the information from such an incident should be restricted to nominated members of the leadership team.
- Possible scenarios might include:
  - Allegations against members of staff.
  - Computer crime – for example hacking of academy systems.
  - Allegations or evidence of 'grooming'.
  - Allegations or evidence of cyber bullying in the form of threats of violence, harassment or a malicious communication.
- Acting 'in loco parentis' and liaising with websites and social media platforms such as Twitter and Facebook to remove instances of illegal material or cyber bullying.

Teaching and teaching support staff:

- Teaching and teaching support staff need to ensure that they are aware of the current academy e-safety policy, practices and associated procedures for reporting e-safety incidents. This is detailed in the 'e-safety, data protection and computer rules summary' document. (this is published annually to teachers)
- All staff need to ensure that they have read, understood and signed (thereby indicating an agreement) the Acceptable Use Policies relevant to internet and computer use in academy.
- All teaching staff need to rigorously monitor pupil internet and computer usage in line with the policy. This also includes the use of personal technology such as cameras, phones and other gadgets on the academy site.
- Teaching staff should promote best practice regarding avoiding copyright infringement and plagiarism.
- Internet usage and suggested websites should be pre-vetted and documented in lesson planning.

Pupils:

- Are required to use academy internet and computer systems in agreement with the terms specified in the academy Acceptable Use Policies. Pupils are expected adhere to this policy when they log onto the internet.
- Pupils need to be aware of how to report e-safety incidents in the academy, and how to use external reporting facilities, such as the CEOP report abuse button.
- Pupils need to be aware that the academy Acceptable Use Policies cover all computer, internet and gadget usage in the academy, including the use of personal items such as phones.
- Pupils need to be aware that their internet use out of academy on social networking sites such as Facebook is covered under the Acceptable Use Policy if it impacts on the academy and/or its staff and pupils in terms of cyber bullying, reputation or illegal activities.

Parents and Guardians:

- It is hoped that parents and guardians will support the academy's stance on promoting good internet behaviour and responsible use of IT equipment both at academy and at home.
- The academy will provide opportunities to educate parents with regard to e-safety.

How will the academy provide e-safety education?

Pupils – curriculum teaching:

- E-safety is an PD teaching unit in year 7; in this unit students learn how to judge the validity of website information, how to remove cyber bullying, computer usage and the law.
- E-safety advice is published on the home group powerpoint and is visible when students log on to the computer system.
- E-safety as a PSHE annual teaching unit: how to deal with cyber bullying, how to report cyber bullying, the social effects of spending too much time online.

Parents – information, presentation, collaborative meetings and events:

- E-safety information is directly delivered to parents via information on the Academy's website and an email to parents. Advice is also given in the termly newsletters
- Twilight courses run by the academy for parents and wider academy community stakeholders.

Staff – inset and training:

- E-safety information directly delivered to staff via twilight sessions and information in staff bulletin.
- A planned calendar programme of e-safety training opportunities is made available for staff depending on role, including on site inset, whole staff training, online training opportunities.
- The e-safety policy will be updated and evaluated by staff at the beginning of each academic year.
- The e-safety Officer should be the first port of call for staff requiring e-safety advice.

Governors – training:

- E-safety information directly delivered to governors via staff bulletins and information published on the academy website.
- Opportunity to attend twilight training with school staff.

ICT support staff – contractors, filtering and monitoring:

- E-safety information directly delivered to support staff via staff bulletin and information on the academy website.
- IT technical support staff and network managers should have relevant industry experience and Microsoft/Cisco certified qualifications.

Particular behaviour which will be highlighted might include:

- Explaining why harmful or abusive images on the internet might be inappropriate or illegal.
- Explaining why accessing age inappropriate, explicit, pornographic or otherwise unsuitable or illegal videos is harmful and potentially unsafe.
- Explaining how accessing and / or sharing other people's personal information or photographs might be inappropriate or illegal.
- Teaching why certain behaviour on the internet can post an unacceptable level of risk, including talking to strangers on social networking; how to spot an unsafe situation before it escalates, and how illegal practises such as grooming can develop.
- Exploring in depth how cyber bullying occurs, how to avoid it, how to stop it, how to report it and how to deal with the consequences of it.
- Teaching pupils to assess the quality of information retrieved from the internet, including recognising how reliable, accurate and relevant information is – particularly information obtained from search engines.
- Informing pupils and staff of copyright and plagiarism infringement laws, and potential consequences with regard to copying material for homework and coursework, copying photographs and images on social networking sites, copying material for using in teaching materials, downloading music, video, applications or other software files illegally.
- Encouraging responsible and effective digital literacy skills which extend beyond academy and into the workplace.
- The medical and social effects of spending too much time on the internet, games consoles or computers.

Use of IT facilities for curriculum teaching and learning:

Use of the internet and IT facilities should be clearly planned prior to the activity. Websites should be suggested, and provided by bookmarks or 'beamed' screens via classroom management software. Students should be trusted to be responsible when researching the internet, but the filtering software needs to be flexible enough to allow teaching staff to manually filter by category as well as specific site depending on the age and maturity of the students.

How to deal with e-safety incidents – action to take:

If illegal material is found on the network, or evidence logged to suggest that illegal material has been accessed

- If the illegal material image is (or is suspected to be) a:
  - Child sexual abuse images hosted anywhere in the world
  - A non-photographic child sexual abuse images hosted in the UK
  - Or a criminally obscene adult content hosted in the UK
- The child protection officer will contact the local police. Follow the academy's child protection procedures if a child protection incident is suspected but: will not copy, archive, forward, send or print out the image – they will leave it in situ, and if in doubt seek advice from the IWF or your local police.

If there is a child protection issue:

If there is a child protection issue, the academy and Child Protection policy will apply.

If there is illegal material which you is unable to be removed which involves Grooming, or suspected child abuse via the internet
The child protection officer will call the local police. They will also contact CEOP http://www.ceop.police.uk/safety-centre/ who have an excellent record for removing such material quickly.

How to deal with e-safety incidents – indicative sanctions for pupils and/or staff:

1 - Illegal activities:

- The Principal or delegated SLT with responsibility for pupil behaviour will deal with the matter.
- The Police and/IWF/CEOP should be contacted if appropriate. Child Protection procedures take precedence over AUPs if CP is a factor.
- The Network Manager, Academy IT Support or external IT contractor (if outside filtering services are used, for example) should be contacted to obtain further evidence.

2 - Going on the internet in lessons or using websites not relevant to the lesson in lesson time:

- The class teacher or personal tutor will deal with the matter and write up an incident report to submit to the e-safety Coordinator / Officer if they are illegal websites.
- The pupil will receive a warning and sanction, as defined in the AUP policy.

3 - Bypassing the academy's filtering system:

- The class teacher or personal tutor will deal with the matter and write up an incident report to submit to the e-safety Coordinator / Officer if appropriate.
- The Network Manager, Academy IT Support should be contacted to obtain further evidence.
- Depending on the severity of the incident parents or carers will need to be informed.
- The Principal or delegated SLT with responsibility for pupil behaviour will deal with the matter.
- The person involved will lose access to the network and/or internet as per the AUP agreement.
- The person will receive a sanction, as defined in the AUP policy.

4 - Viewing pornographic material:

- The class teacher or personal tutor will deal with the matter and write up an incident report to submit to the e-safety Coordinator / Officer if appropriate.
- The Network Manager, Academy IT Support should be contacted to obtain further evidence.
- The Police and IWF should be contacted if indecent material was uploaded or downloaded. CEOP should be contacted if grooming / sexting or unwanted sexual advances were involved.
- The Principal or delegated SLT with responsibility for pupil behaviour will deal with the matter.
- Parents or carers will need to be informed.
- The person involved will lose access to the network and/or internet as per the AUP agreement.
- The person will receive a sanction, as defined in the AUP policy.

5 - Using social media (Twitter and Facebook) or email in lesson time:

- The class teacher or personal tutor will deal with the matter and write up an incident report to submit to the e-safety Coordinator / Officer if appropriate.
- The Network Manager, Academy IT Support should be contacted to obtain further evidence.
- Depending on the severity of the incident parents or carers will need to be informed.
- The Principal or delegated SLT with responsibility for pupil behaviour will deal with the matter.
- The person involved will lose access to the network and/or internet as per the AUP agreement.
- The person will receive a sanction, as defined in the AUP policy.

6 - Cyber bullying:

- The class teacher or personal tutor will deal with the matter and write up an incident report to submit to the e-safety Coordinator / Officer if appropriate.
- The Network Manager, Academy IT Support should be contacted to obtain further evidence.
- Depending on the severity of the incident parents or guardians will need to be informed.
- The Principal or delegated SLT with responsibility for pupil behaviour will deal with the matter.
- The person involved will lose access to the network and/or internet as per the AUP agreement.
- The person will receive a sanction, as defined in the AUP policy.

7 - Writing malicious comments about the academy or bringing the academy name into disrepute – whether in academy time or not:

- The class teacher or personal tutor will deal with the matter and write up an incident report to submit to the e-safety Coordinator / Officer if appropriate.
- The Network Manager, Academy IT Support should be contacted to obtain further evidence.
- Depending on the severity of the incident parents or guardians will need to be informed.
- The Principal or delegated SLT with responsibility for pupil behaviour will deal with the matter.
- The person involved will lose access to the network and/or internet as per the AUP agreement.
- The person will receive a sanction, as defined in the AUP policy.

8 - Deleting someone else's work or unauthorised deletion of academy files:

- The class teacher or personal tutor will deal with the matter and write up an incident report to submit to the e-safety Coordinator / Officer if appropriate.
- The Network Manager, Academy IT Support should be contacted to obtain further evidence and if possible restore the deleted work.
- The Principal or delegated SLT with responsibility for pupil behaviour will deal with the matter.
- The person involved will lose access to the network and/or internet as per the AUP agreement.
- The person will receive a sanction, as defined in the AUP policy.

9 - Uploading or downloading inappropriate or illegal files using the academy network:

- The class teacher or personal tutor will deal with the matter and write up an incident report to submit to the e-safety Coordinator / Officer if appropriate.
- The Network Manager, Academy IT Support should be contacted to obtain further evidence.
- Depending on the severity of the incident parents or guardians will need to be informed.
- The Principal or delegated SLT with responsibility for pupil behaviour will deal with the matter.
- The person involved will lose access to the network and/or internet as per the AUP agreement.
- The person will receive a sanction, as defined in the AUP policy.

10 - Copyright infringement of text, software or media:

- The class teacher or personal tutor will deal with the matter and write up an incident report to submit to the e-safety Coordinator / Officer if appropriate.
- The Network Manager, Academy IT Support should be contacted to obtain further evidence.
- Depending on the severity of the incident parents or guardians will need to be informed.
- The Principal or delegated SLT with responsibility for pupil behaviour will deal with the matter.
- The person involved will lose access to the network and/or internet as per the AUP agreement.
- The person will receive a sanction, as defined in the AUP policy.

APPENDIX One

E-safety and the Law:

Computer Misuse Act 1990, sections 1-3
GDPR
Freedom of Information Act 2000
Communications Act 2003 section 1,2
Protection from Harassment Act 1997
Regulation of Investigatory Powers Act 2000
Copyright, Designs and Patents Act 1988
Racial and Religious Hatred Act 2006
Protection of Children Act 1978
Sexual Offences Act 2003

The Education and Inspections Act 2006 (Head teachers have the power "to such an extent as is reasonable" to regulate the conduct of pupils off site. Also, staff can confiscate mobile phones if they cause disturbance in class breach the academy behaviour policy.)

Duty of care and 'in loco parentis':

Academies have a 'duty of care' to pupils, and as such act "in loco parentis." Under the Children Act 1989, this enables academies to remove personal information, cyber bullying and comments relating to academy pupils as if they were the child's parent. Facebook in particular has provision for using 'in loco parentis' when reporting cyber bullying. This is relevant to all academies, but especially to boarding and residential academies.

Specific academy policies to support good practice in e-safety:

Acceptable Internet Usage Policy:

- The academy Acceptable Usage Policy covers use by pupils, staff and other adults working in academy and also the usage of academy related internet technologies such as extranets, E-Learning platforms, website, social media and external network logins.
- The purpose and scope of the E-Learning Policies are explained to those required to sign and agree to them by means of a presentation and opportunity to ask questions. New pupils will be informed of the scope and purpose of the AUPs as part of induction prior to joining the academy, or at the start of their first term.
- It is assumed that pupils and staff will not be granted access to academy internet and related internet technologies until the AUP agreement has been discussed.

E-safety and computer security rules summary booklet:

- The academy's computer security and e-safety booklet is designed a summary of the e-safety policy and security rules.

Data protection policy:

- The data protection policy is designed to outline to staff and other stake holder the implications of breaching the DPA act 1998.
- It is designed to ensure that all staff within the academy are complying with the law in regards to data held by the academy on pupils and parents.

APPENDIX Two

E-safety in practice - Guidance for Senior Leadership Team

Systems:

- Academy computer systems are firstly fit for purpose, and secondly customised to ensure e-safety. For pupil machines, the primary purpose is to ensure the configuration of academy computers, networks and file-serving is designed to meet the teaching and learning requirements of the academy. e-safety is then be fully implemented without sacrificing the teaching and learning requirements and functionality.
- It is not acceptable or best practice for network managers to design a system based to facilitate easy implementation of e-safety, monitoring and security systems firstly, with pupils and staff having to then work around an ill-fitting network not best suited to delivering effective teaching and learning.
- Network managers should always take into account the needs of the users – ie the pupils and teachers. It is the responsibility of the network manager to implement e-safety effectively without restricting or altering the requirements of the users. A creative and can-do approach is essential.
- Network managers should always ensure that academy, LA, DfE, ICO, Data Protection and TA guidelines with regard to e-safety are met and implemented.
- Network managers need to carry out regular audits and evaluations of the academy IT network and should maintain a ongoing development plan for IT provision.
- The key e-safety aims with regard to computer systems, access, file-serving and networking are to create a system which can log, track and evidence e-safety events, and provide data to enable accurate evaluation and improvements to be made. This needs to be borne in mind when justifying any decision regarding e-safety and network design and implementation.
- Network managers need to create a system where every login, data transaction, or other activity can be logged, traced to a particular user and monitored in the event of abuse.
- Servers, network switches, hubs, Cat5 or Fibre Optic cabling, wireless transmitters, bridges, access points and other physical architecture should be secured to prevent unauthorised or untraceable network access.

Filtering:

- The filtering provider should be the first port of call for advice regarding filtering. It is best practice if they provide the basis for a filtering policy, based precisely on the system and settings in operation for the academy. If generic or inaccurate policies are used, a misleading impression of the filtering process and logging capability can be created. It is not advisable to purchase a package or subscribe to an external contractor if they are unable to provide this information and in the form the academy requires. Maintained sector academies will have access to GfL filtering via their broadband consortium or LA. Detailed polices will be provided by the LA and should be adopted without any significant alteration.
- The academy's internet service must be provided by a fully accredited ISP. Accredited filtering should be used. The academy must be able to differentiate the levels of filtering based on pupil age, maturity, responsibility; and staff use. The filtering reports and logs should be examined daily, and if possible there should be a facility to monitor 'on the fly'. Classroom management systems should be utilised by teaching staff to monitor all pupils screens on one staff screen or IWB. Any alterations to the filtering protocol are authorised, recorded and reasons provided. Any filtering 'incidents' are examined and action is taken and recorded to prevent a reoccurrence.
- Filtering and monitoring needs to reflect real life rather than being a 'lock down' system. If locked down, or white-list only, the academy risks simply transferring e-safety problems incidents elsewhere – for example to mobile phones, or home usage. The problem isn't being dealt with and good behaviours are not being taught. Pupils need to be taught positive responsible behaviour to carry forward into the workplace.

Monitoring:

- The academy installed monitoring package (software or hardware) manufacturer or provider should be your first port of call regarding capabilities and procedures. It is best practice to use a monitoring solution which includes an exemplar procedure for monitoring and logging activity. Generic policies are not advised since no two monitoring packages are the same. To achieve the academy's precise e-safety aims may require the use of more than one monitoring and logging package.

Network security:

Passwords:

- The use of network profiles which require the user to input a username and password is one way to enable the network manager to log network and internet activity specific to a user, in order to fulfil e-safety requirements.
- There are flaws with this approach which the network manager will need to consider carefully. Firstly, passwords can be shared. Secondly, pupils might work in pairs or small groups, thirdly computers can be left logged on and as a result another user could cause an e-safety incident which could be incorrectly attributed to the wrong person.
- Also, there may be teaching and learning requirements which necessitate collaborative learning, shared access to group work, paired work or peer review tasks which require more than one user to access the same file, workstation or internet browsing – rendering a user profile logging approach ineffective and unconstructive to teaching and learning.
- Furthermore, with younger children and older machines, requiring all pupils to switch machines on and log in prior to the teacher beginning the lesson can take a significant amount of time – in some cases up to seven minutes – which is unacceptable for teaching and learning. Best practice for teaching and learning is to create a situation where all technology is "ready to go" prior to the students entering the room. It is not always possible to achieve this with network wide profile logins.
- The academy password policy needs to be configured with the assistance of the Network Manager to ensure:
- A password history is kept so that old passwords are not re-used.
- Passwords expire after a set number of days – and not in the holidays - otherwise the first day of term is chaos.
- Passwords have a minimum and maximum length, to prevent 'easy' passwords or mistakes when creating passwords.
- Passwords must meet complexity requirements – ie they need to be 'strong' passwords, for example using upper and lower case letters, numbers and symbols.
- Passwords should be stored using non-reversible encryption – in other words there should not be a great big text file with all the passwords for pupils to find on the network – passwords should be encrypted.
- Pupils and staff should be encouraged to change passwords – for all important accounts, and not just academy profiles – regularly.
- Backups should be made to encrypted fileservers or partitions – to prevent an individual walking away with an entire academy network on a portable hard-drive. If cloud services are used, the TOS of the cloud host need to be scrutinised extremely carefully given the ICO requirements for storage of "personal data". Generally, cloud backup services are not advised for personal data.