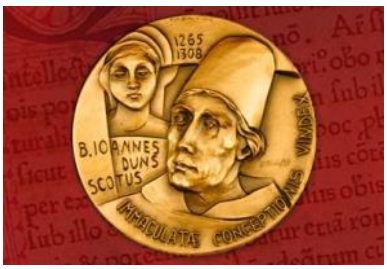
St Luke Academies Trust

ICT and Acceptable Use Policy



Adopted: January 2016

Review Date: January 2017

Our Lady Of Walsingham Catholic Primary School

ICT and Acceptable Use Policy

1. Introduction

In order to create a safe teaching and learning environment, effective policies and procedures which are clearly understood and followed by the whole school community are essential. This Acceptable Use Policy sets out the roles, responsibilities and procedures for the safe and appropriate use of all technologies to safeguard adults, children and young people within Our Lady Of Walsingham Catholic Primary School. This policy should be read in conjunction with the Child Protection and Safeguarding Policy. The policy recognises the ever changing nature of emerging technologies and highlights the need for regular review to incorporate developments within ICT.

The purpose of the Acceptable Use Policy is to clearly identify for the whole school community:

i) the steps taken in school to ensure the safety of pupils when using the internet, e-mail and related technologies

ii) the school's expectations for the behaviour of the whole school community whilst using the internet, e-mail and related technologies within and beyond school

iii) the school's expectations for the behaviour of staff when accessing and using data.

2. The aims of this policy

- To ensure the safeguarding of all children and young people within and beyond the school setting by detailing appropriate and acceptable use of all on-line technologies.
- To outline the roles and responsibilities of everyone.
- To ensure adults are clear about procedures for misuse of any on-line technologies both within and beyond the school setting.
- To develop links with parents/carers and the wider community ensuring input into policies and procedures with continued awareness of benefits and potential issues of on-line technologies.
- To outline our approach to planning, teaching and assessment in ICT.

3. Responsibilities

3.1 Head Teacher and Governors

The Head teacher and Governors have overall responsibility for e-Safety as part of the wider remit of safeguarding and child protection. To meet these responsibilities, the Head Teacher and Governors should:

- designate an e-Safety Lead (normally this will be the ICT subject leader) to implement agreed policies, procedures, staff training, curriculum requirements and take the lead responsibility for ensuring e-Safety is addressed appropriately. All employees, students and volunteers should be aware of who holds this post within school.
- provide resources and time for the e-Safety lead and employees to be trained and update protocols where appropriate.
- promote e-safety across the curriculum and have an awareness of how this is being developed, linked with the school development plan.
- share any e-safety progress and curriculum updates at all governing body meetings and ensure that all present understand the link to child protection.
- ensure that e-safety is embedded within all child protection training, guidance and practices.
- elect an e-Safety Governor to challenge the school about e-Safety issues.
- make employees aware of the LSCBN Inter-agency Child Protection Procedures at www.lscbnorthamptonshire.org.uk

3.2 E-Safety Lead

The nominated e-Safety lead should:

- recognise the importance of e-Safety and understand the school's duty of care for the-Safety of their pupils and employees.
- establish and maintain a safe ICT learning environment within the school.
- ensure that all individuals in a position of trust who access technology with students understand how filtering levels operate and their purpose.
- with the support of the Network Manager, ensure that filtering is set to the correct level for employees, young volunteers, children and young people accessing school equipment.
- report issues of concern and update the Head Teacher on a regular basis.

- liaise with the Anti-Bullying, and child protection leads so that procedures are updated and communicated, and take into account any emerging e-safety issues and technological changes.

- co-ordinate and deliver employee training according to new and emerging technologies so that the correct e-Safety information is being delivered.

- maintain an e-Safety Incident Log to be shared at agreed intervals with the Head Teacher and Governors at governing body meetings.

- with the support of the Network Manager, implement a system of monitoring employee and pupil use of school issued technologies and the internet where appropriate.

-

3.3 Individual Responsibilities

All school based employees, including volunteers under the age of 18, must:

- take responsibility for their own use of technologies and the internet, making sure that they are used legally, safely and responsibly.

- ensure that children and young people in their care are protected and supported in their use of technologies so that they can be used in a safe and responsible manner. Children should be informed about what to do in the event of an e-Safety incident.

- report any e-Safety incident, concern or misuse of technology to the e-Safety lead or Head Teacher, including the unacceptable behaviour of other members of the school community.

- use school ICT systems and resources for all school related business and communications, particularly those involving sensitive pupil data or images of students. School issued email addresses, mobile phones and cameras must always be used by employees unless specific written permission to use a personal device has been granted by the Head Teacher, for example, due to equipment shortages.

- ensure that all electronic communication with pupils, parents, carers, employees and others is compatible with their professional role and in line with school protocols. Personal details, such as mobile number, social network details and personal e-mail should not be shared or used to communicate with pupils and their families.

- not post online any text, image, sound or video which could upset or offend any member of the whole school community or be incompatible with their professional role. Individuals working with

children and young people must understand that behaviour in their personal lives may impact upon their work with those children and young people if shared online or via social networking sites.

- protect their passwords/personal logins and log-off the network wherever possible when leaving work stations unattended.

- understand that network activity and online communications on school equipment (both within and outside of the school environment) may be monitored, including any personal use of the school network.

- understand that employees, who ignore security advice or use email or the internet for inappropriate reasons, risk dismissal and possible police involvement if appropriate.

3.4 Children and young people

Children and young people are:

- Involved in the review of our Acceptable Use Rules through the school
- council or other appropriate group, in line with this policy being
- reviewed and updated.
- Responsible for following the Acceptable Use Rules whilst within
- school as agreed at the beginning of each academic year or whenever
- a new child attends the school or setting for the first time.
- Taught to use the Internet in a safe and responsible manner.
- 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).

4. Appropriate use

4.1 By staff or adults

Staff members have access to the network so that they can access 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 will receive a copy of the Acceptable Use Policy and a copy of the Acceptable Use Rules, which then need to be signed and kept under file with a signed copy returned to the member of staff. The Acceptable Use Rules 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. 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.

Please refer to appendices for a complete list of Acceptable Rules for Staff.

4.2 By children and young people

Acceptable Use Rules and our letter explaining these to our parents are outlined in the Appendices and detail how they are expected to use the Internet and other technologies within Our Lady Of Walsingham

Primary School. This includes downloading or printing of any materials. The rules are there for our children to understand what is expected of their behaviour and attitude when using the Internet which then enables 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 rules will be on display within our classrooms and anywhere else where this may be applicable.

We want our parents/carers to support our rules with their child. This will be shown by them signing the Acceptable Use Rules together so that it is clear to us that the rules are accepted by each one of our children with the support of the parent/carer. This is also intended to provide support and information to parents/carers when children may be using the Internet beyond school.

4.3 In the event of inappropriate use

Should a child or young person be found to misuse (see Appendix) the on-line facilities whilst at school or in a setting the following consequences will occur

- Any child found to be misusing the Internet by not following the acceptable Use Rules will 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 rules will result in not being allowed to access the Internet for a period of time and another letter will be sent home to parents/carers.
- A letter will be sent to parents/carers outlining the breach in the Child Protection 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 will 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) to make a report and seek further advice. Children will be taught and encouraged to consider the implications for misusing the Internet and posting inappropriate materials to websites, for example, as this can lead to legal implications.

7. The curriculum and tools for Learning

7.1 Internet use

At Our Lady Of Walsingham Catholic Primary School we teach our children and young people how to use the Internet safely and responsibly, for researching information, exploring concepts, deepening knowledge and understanding and communicating effectively in order to further learning. This is done so through Computing and PSHE lessons. By the time our children leave us we expect that they will have an understanding of:

- 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 on-line 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
-

We follow the National Curriculum for computing and each unit of work contains a lesson on safety. These skills and competencies are taught within the curriculum so that children and young people have the security to explore how on-line technologies can be used effectively, but in a safe and responsible manner. Children and young people will know how to deal with any incidents with confidence.

7.2 Mobile phones and other technologies

We carefully consider how the use of mobile technologies can be used as a teaching and learning tool within the curriculum, taking into consideration the following areas of concern:

- inappropriate or bullying text messages
- images or video taken of adults or peers without permission
- being sought
- 'happy slapping' – the videoing of violent or abusive acts towards a child, young person or adult which is often distributed

The use of mobile phones is not allowed by our children in our school during school hours. The same rules of acceptable use will apply to mobile phone users. **Staff members are not allowed to use their personal numbers to contact children and young people under any circumstances.** It is also our policy to ensure that we educate our children and young people in understanding the use of a public domain and the consequences of misusing it including the legal implications and law enforcement through relevant curriculum links.

7.3 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 there is access to digital cameras and recorders. Members of staff are not allowed to use their own equipment without express authorisation from the ICT Subject Manager. We always check with parents/carers prior to any uploading of images. The sharing of photographs via weblogs, forums or any other means on-line will only occur after permission has been given by a parent/carer or member of the School Leadership Team. Any photographs or video clips uploaded should not have a file name of a child, especially where these may be uploaded to a school website. Photographs should only ever include the child's first name. Any such photographs will be stored on the school's central computer.

8 Curriculum Organisation

The school uses the National Curriculum for computing to develop our curriculum. Teaching staff annotate these to suit their own class and the particular aspect of the curriculum that they are teaching.

Assessment is built into this scheme and is completed after each unit has been taught.

Computing skills are also incorporated into other aspects of our curriculum and children are encouraged to use computers as much as possible when recording their work.

Appendices

Staff Procedures Following Misuse by Staff

The Headteacher will ensure that these procedures are followed, in the event of any misuse of the Internet, by an adult:

A. *An inappropriate website is accessed inadvertently:*

Report website to the e-Safety Leader if this is deemed necessary. Contact the helpdesk filtering service and LA/RBC so that it can be added to the banned or restricted list. Change Local Control filters to restrict locally. Check the filter level is at the appropriate level for staff use in school.

B. *An inappropriate website is accessed deliberately*:

Ensure that no one else can access the material by shutting down. Log the incident. Report to the Headteacher and e-Safety Leader immediately. Headteacher to refer back to the Acceptable Use Rules and follow agreed actions for discipline. Inform the LA/RBC filtering services as with A.

C. *An adult receives inappropriate material.*

Do not forward this material to anyone else – doing so could be an illegal activity. Alert the Headteacher immediately. Ensure the device is removed and log the nature of the material. Contact relevant authorities for further advice e.g. police.

D. *An adult has used ICT equipment inappropriately:*

Follow the procedures for B.

E. *An adult has communicated with a child or used ICT equipment inappropriately:*

Ensure the child is reassured and remove them from the situation immediately, if necessary. Report to the Headteacher and Designated Person for Child Protection immediately, who should then follow the Allegations Procedure and Child Protection Policy. Preserve the information received by the child if possible and determine whether the information received is abusive, threatening or innocent. Once Procedures and Policy have been followed and the incident is considered innocent, refer to the Acceptable Use Rules for Staff and Headteacher to implement appropriate sanctions. If illegal or inappropriate misuse is known, contact the Headteacher or Chair of Governors (if allegation is made against the Headteacher) and Designated Person for Child Protection immediately and follow the Allegations procedure and Child Protection Policy. Contact CEOP (police) as necessary.

F. *Threatening or malicious comments are posted to the school website about an adult in school:*

Preserve any evidence. Inform the Headteacher immediately and follow our Child Protection Policy as necessary. Inform the RBC/LA/LSCBN and e-Safety Leader so that new risks can be identified. Contact the police or CEOP as necessary.

G. Where staff or adults are posted on inappropriate websites or have inappropriate information about them posted

This should be reported to the Headteacher.

Staff Procedures Following Misuse by Children and Young People

The Headteacher will ensure that these procedures are followed, in the event of any misuse of the Internet, by a child or young person:

A. An inappropriate website is accessed inadvertently:

Reassure the child that they are not to blame and praise for being safe and responsible by telling an adult.

Report website to the e-Safety Leader if this is deemed necessary. Contact the helpdesk filtering service for school and LA/RBC so that it can be added to the banned list or use Local Control to alter within your

setting. Check the filter level is at the appropriate level for staff use in school.

B. An inappropriate website is accessed deliberately:

Refer the child to the Acceptable Use Rules that were agreed. Reinforce the knowledge that it is illegal to access certain images and police can be informed. Decide on appropriate sanction. Notify the parent/carer. Inform LA/RBC as above.

C. An adult or *child has communicated with a child or used ICT equipment inappropriately*:

Ensure the child is reassured and remove them from the situation immediately. Report to the Headteacher and Designated Person for Child Protection immediately. Preserve the information received by the child if possible and determine whether the information received is abusive, threatening or innocent. LSCBN. Contact CEOP (police) as necessary.

D. Threatening or malicious comments are posted to the school website or learning platform about a child in our school:

Preserve any evidence. Inform the Headteacher immediately. Inform the RBC/LA/LSCBN and e-Safety Leader so that new risks can be identified. Contact the police or CEOP as necessary.

E. Threatening or malicious comments are posted on external websites about an adult in our school:

Preserve any evidence. Inform the Headteacher immediately.

N.B. There are three incidences when you must report directly to the police.

- Indecent images of children found.
- Incidents of 'grooming' behaviour.
- The sending of obscene materials to a child.
-

CEOP advice is to turn off the screen, secure the machine and contact the police for further instructions if an indecent image is found. They will advise on how to deal with the machine, if they are unable to send out a forensics team immediately. If in doubt, do not power down the machine. Grabbing a screenshot is not a technical offence of distribution, but of 'making' an image.

• www.iwf.org.uk will provide further support and advice in dealing with offensive images on-line.

It is important to remember that any offensive images that may be received should never be forwarded to anyone else, even if it is to report them as illegal as this constitutes illegal activity and the person forwarding the images will be liable to prosecution and investigation by the police.

Acceptable Use Rules for Staff

These rules apply to all on-line use and to anything that may be downloaded or printed. To ensure that all adults within our school are aware of their responsibilities when using any on-line technologies, such as the Internet or E-mail, they are asked to sign the Acceptable Use Rules below. This is so that they provide an example to children and young people for the safe and responsible use of on-line technologies which will educate, inform and protect and so that they feel safeguarded from any potential allegations or inadvertent misuse themselves.

Acceptable Use Rules for members of staff.

- I know that I should only use the school equipment in an appropriate manner and for professional uses.
- I understand that I need to give permission to children and young people before they can upload images (video or photographs) to the Internet or send them via E-mail.
- I know that images should not be inappropriate or reveal any personal information of children and young people if uploading to the Internet.
- I have read the Procedures for Incidents of Misuse so that I can deal with any problems that may arise, effectively.
- I will report accidental misuse.
- I will report any incidents of concern for children's or young people's safety to the Headteacher, Designated Person for Child Protection or e-Safety Leader in accordance with procedures listed in the Acceptable Use Policy.
- I know who my Designated Person for Child Protection is.
- I know that I am putting myself at risk of misinterpretation and allegation should I contact children and young people via personal technologies, including my personal e-mail and should use the school E-mail and phones (if provided) and only to a child's school E-mail address upon agreed use within the school.
- I know that I should not be using the school system for personal use unless this has been agreed by the Headteacher and/or e-Safety Leader.
- I know that I should complete virus checks on my laptop and memory stick or other devices so that I do not inadvertently transfer viruses, especially where I have downloaded resources.
- I will only install hardware and software on school equipment I have been given permission for.
- I will ensure that I follow the Data Protection Act 1998 and have checked I know what this involves.
- I will ensure that I keep my password secure and not disclose any security information unless to appropriate personnel. If I feel someone inappropriate requests my password I will check with the e-Safety Leader.
- I have been given a copy of the Acceptable Use Policy to refer to about all e-safety issues and procedures that I should follow.
- I will adhere to copyright and intellectual property rights.

I have read, understood and agree with these Rules as I know that by following them I have a better understanding of e-Safety and my responsibilities to safeguard children and young people when using on-line technologies.

Signed…….Date…….

Name (printed)…….

Further Information and Guidance

The nature of e-safety is evolving. Encourage safe practice. You may want to keep up to date with further supporting documents, information or advice, which can be found on:

- www.parentscentre.gov.uk (for parents/carers)
- www.ceop.co.uk (for parents/carers and adults)
- www.iwf.org.uk (for reporting of illegal images or content)
- www.thinkuknow.co.uk (for all children and young people with a section for parents/carers and adults – this also links with the CEOP (Child Exploitation and On-line Protection Centre work)
- www.netsmartzkids.org (5 – 17)
- www.kidsmart.org.uk – (all under 11)
- www.phonebrain.org.uk (for Yr 5 – 8)
- www.bbc.co.uk/cbbc/help/safesurfing (for Yr 3/4)
- www.hectorsworld.com (for FS, Yr 1 and 2 and is part of the thinkuknow website above)
- www.teachernet.gov.uk (for schools and settings)
- www.dcsf.gov.uk (for adults)
- www.digizen.org.uk (for materials from DCSF around the issue of cyber bullying)
- www.becta.org.uk (advice for settings to update policies) and
- http://www.nextgenerationlearning.org.uk/esafetyandwifi.html (simple tips for parents/adults)
- http://www.northamptonshire.gov.uk/NACPC/acpc_home.htm (Local Safeguarding Children's Board Northamptonshire – policies, procedures and practices, including Section 12 of the Allegations Procedures are available here)
- www.nen.org.uk (for schools and settings – access to the National Education Network)