Longford Primary Academy

Member of staff responsible: Vice Principal
Safeguarding governor: Michelle Williams
Date Policy Written: Autumn 2018
Date approved by the full governing body:
Date to be reviewed: Autumn 2019

Online safety Policy

(Incorporating ICT Security Policy)

Policy Statement

At Longford we recognise the contribution modern technologies makes to the curriculum and life itself. Our aim is to provide a safe and secure environment where children and adults can experience and develop their computer skills and enhance learning across the curriculum.

AIMS:

- Enable children to make appropriate, safe and informed choices about their use of technologies
- Provide a safe and non-threatening environment for learning, which has the flexibility to meet the individual needs and abilities of each pupil
- To maintain a safe and secure environment in which to learn both on-line and off-line, taking into account all new mobile learning devices
- To protect children from harm by ensuring the appropriate management and use of emerging technologies
- To safeguard children by promoting appropriate and acceptable use of digital imagery
- To minimise risk and safeguard the professional reputation of staff and that of Longford Primary School

ROLES AND RESPONSIBILITIES

Principal & SLT

The Principal is responsible for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to the e-safety co-ordinator. The Principal should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.

Governors

Governors are responsible for the approval of the e-safety policy and for reviewing the effectiveness of the policy.

E-safety co-ordinator

The e-safety co-ordinator is responsible for the development and implementation of the e-safety policy across the school. It is important that the e-safety co-ordinator remains up-to-date with new developments, issues and threats to the safety of the pupils and staff whilst online. The e-safety co-ordinator:

- ensures the e-safety policy is implemented consistently throughout the school

- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies/documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments
- ensures the safety of equipment

Technical Staff

The technician e-safety co-ordinator are responsible for ensuring:

- that the school's infrastructure is secure and is not open to misuse or malicious attack
- that the school meets the e-safety technical requirements outlined in the Entrust Security Policy and Acceptable Usage Policy (AUP) and any relevant LA e-safety policy and guidance
- that users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed
- that he/she keeps up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant
- that the use of the network/Virtual Learning Environment (VLE)/email is regularly monitored in order that any misuse/attempted misuse can be reported to the e-safety co-ordinator for investigation.
- that monitoring software/systems are implemented and updated as agreed in school policies. Longford Primary uses:
    - ✓ Netsweeper: Internet filtering service. This is a specialised web-filtering product designed for education.
    - ✓ PCE/Future cloud: Recommended e-safety solution by entrust learning technologies. This monitors pupils when they use ICT and captures behavioural risks that would otherwise go undetected.
    - ✓ Symantec: provides internet security with Norton AntiVirus, data recovery, and spam blocker software. This operates both on school site and at home for staff members who use their laptops at home.

Classteacher

- To ensure that they and all pupils have signed relevant e-safety forms and that e-safety issues are addressed and adhered to. Breeches of security/misuse should be reported to the e-safety co-ordinator who will issue a written letter to parents.
- They have an up to date awareness of e-safety matters and of the current school e-safety policy and practices
- They have read, understood and signed the school staff Acceptable Use Agreement (AUA)
- Digital communications with pupils should be on a professional level and only carried out using official school systems
- Pupils understand and follow the school e-safety and AUA

- In lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
- To make children aware of the dangers and misuse of new technologies and teach them how to use these technologies safely through a planned e-safety program (see skills ladder/curriculum map)

Designated person for child protection
Should be trained in e-safety issues and be aware of the potential for serious child protection issues to arise from:

- sharing of personal data
- access to illegal/inappropriate materials
- inappropriate on-line contact with adults/strangers
- potential or actual incidents of grooming
- cyber-bullying

N.B. These are child protection issues, not technical issues, it is simply that the technology provides additional means for child protection issues to develop.

Parents/Carers
Parents/Carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website/VLE and information about e-safety.

Parents and carers will be responsible for:

- Endorsing (by signature) the AUA/code of conduct
- Accessing the school website/VLE in accordance with the relevant school AUA.

CURRICULUM

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages in the use of learning technologies across the curriculum.

- In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, eg using search engines, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that these sites can be temporarily removed from the filtered list for the period of study.

Longford Primary Academy

E-safety education will be provided in the following ways:

For pupils:

- A planned e-safety programme will be provided as part of computing/PHSE/ other lessons and should be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school. In line with the schools thematic approach lessons will be taught in a relevant and meaningful way whilst also building upon each other by reinforcing developmentally appropriate topics, such as using letters of the alphabet to search and following rules to remain safe in EYFS to exploring cyberbullying, talking safely on-line and responsible use as children progress thoughout the school, with the aim being that children at Longford know what it means to be a good digital citizen. The curriculum will cover aspects of:
    - ✓ internet safety
    - ✓ privacy and security
    - ✓ relationships and communication
    - ✓ cyberbullying
    - ✓ digital footprints and reputation
    - ✓ self-image and identity
    - ✓ information literacy
    - ✓ creative credit and copyright

NB. See skills ladder/i-Compute scheme of work for a more detailed curriculum map

- Key e-safety messages should be reinforced as part of a planned programme of assemblies and pastoral activities
- Pupils should be helped to understand the need for the pupil AUA and encouraged to adopt safe and responsible use of communication technologies, the internet and mobile devices both within and outside school
- Rules for use of technology systems/internet will be posted in all rooms
- Staff should act as good role models in their use of communication technologies, the internet and mobile devices

For parents/carers:

Many parents and carers have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring of the children's on-line experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. "There is a generational digital divide". (Byron Report).

The school will therefore seek to provide information and awareness to parents and carers through:

- Letters, newsletters and website
- Parents evenings
- Workshops

- Parents and carers will be reminded that they must not share, distribute or display images containing other children without the relevant permission or consent from their parents (via annual AUA and verbally at school events such as plays, concerts and sports days)

For staff:
It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy.

- An audit of the e-safety training needs of all staff will be carried out regularly.
- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Policies
- The e-safety coordinator will receive regular updates through attendance at training sessions and by reviewing guidance documents released by BECTA/LA and others.
- This e-safety policy and its updates will be presented to and discussed by staff in staff meetings/INSET days.
- The e-safety coordinator will provide advice & guidance to individuals as required
- All staff (including students) should be made aware of and understand the need for an AUA (which will be endorsed by signature) and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school

For Governors:
Governors should take part in e-safety training/awareness sessions, with particular importance for those who are members of any sub-committee involved in ICT/e-safety/health and safety/child protection.

CHILDREN'S RECORDS (LEARNING JOURNEYS/PROFILES/ASSESSMENT RECORDS)

Legislative framework:

- **Data Protection Act (1998)**
- **Freedom of Information Act (2000)**
- **Statutory Framework for the Early Years Foundation Stage (2012)**

Procedures

- Permission must be obtained from parents/carers for learning journeys to be stored on a secure online profile programme (Tapestry).
- All websites and iPads used to access this program must be password protected.
- Learning journeys (both paper and online) are to be treated as personal data as each learning journey relates to an individual, identifiable child.
- Consent will be requested from parents/carers for group images to be included in the learning journeys of other children as well as standard individual annual consent. On request, parents and carers must be given the opportunity to view any images before they are included in any images before they are included in any learning journey and must be given the option to restrict their consent.
- If it is not possible to obtain consent, the relevant images must not be shared across learning journeys of other children.

- Parents and carers must be reminded that they must not share, distribute or display images containing other children without the relevant permission or consent from their parents.
- Parents should be encouraged to contribute information to this learning journey, by including some information and photographs which show what their child enjoys doing at home.
- When children move schools information will be transferred electronically (CTF) via a secure online access site which is password protected.

INTERNET SAFETY

At Longford all student access to the internet is supervised. Pupil code of conduct/AUA letters are signed by all pupils at the beginning of each academic year which are kept in homework dairies (KS2) or a class file (KS1) along with photographic and other permissions forms (see appendix 1 & 2). All staff (including visiting students and helpers) must also complete an AUA & code of conduct, which are kept on file by the Vice principal (see appendix 4).

At Longford we aim to educate learners to use the system responsibly and safely. We use a filtered service through Netsweeper. This filtering intercepts an unsuitable request by any user and refers to a regularly updated list of blocked sites before allowing access.

Pupils will be taught to search the internet safely and through appropriate search engines such as KidRex. **No pupil should be given an open search on google.** Sites that have been thoroughly researched by staff may be bookmarked and stored into shared links or directed through a word document. Pupils should be taught in all lessons to be critically aware of the content they access on-line and be guided to validate the accuracy of information.

Communications

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

E-mail

- pupils may only use approved e-mail accounts on the school system.
- pupils must immediately tell a teacher if they receive offensive e-mail.
- pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone.
- the same level of professional language and content applies to e-mail sent to external organizations
- The official school email service may be regarded as safe and secure and is monitored. Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school systems (eg by remote access).
- Users need to be aware that email communications may be monitored
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.

- Any digital communication between staff and pupils or parents/carers (email, chat, VLE etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or public chat/social networking programmes must not be used for these communications.
- Where possible, whole class or group email addresses will be used at KS1, while pupils at KS2 and above will be provided with individual school email addresses for educational use.
- Pupils should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.

School website

- the contact details on the website should be the school address, e-mail and telephone number. Staff or pupils' personal information is not published
- the Principal has overall editorial responsibility for the website and ensures that content is accurate and appropriate.
- photographs that include pupils are selected carefully so they do not enable individual pupils to be clearly identified.
- pupils' full names are not used anywhere on the website,
- photographs of children will only be published on the school website/social media account where parental permissions have been granted,
- pupils' work will only be published with the permission of the pupil and parents
- personal information should not be posted on the school website and only official email addresses should be used to identify members of staff,

School social media account

As above and:

- The Vice principal has overall editorial responsibility for the website and ensures that content is accurate and appropriate.
- contribution rights and restrictions are set by the Vice principal
- the school reserves the right to block parents from the social media account if it is deemed that they have misused the site or bought the school into disrepute via their comments.

Social networking and personal publishing

- the school blocks access to social networking sites.
- newsgroups are also blocked.
- pupils are told never to give out personal details of any kind which may identify them
- pupils and parents are advised that the use of social network spaces outside school is inappropriate for primary aged pupils.
- staff are not permitted to accept pupils as 'friends' and communicate with them through social networking sites such as Facebook. It is considered good practice at Longford that this follows for parents of children attending Longford Primary School (see appendix 3).

- All staff are made vitally aware that posting unsuitable images on social network spaces and unsuitable messages may cause personal embarrassment and may infringe professional integrity of yourself and colleagues (see appendix 3).
- The school adopts the 'Code Of Practice For Employees in the use of Social Networking Sites and Electronic Media' (see appendix 6)

MANAGING EMERGING TECHNOLOGIES

Legislative Framework

- **Data Protection Act (2018)**
- **Freedom of Information Act (2000)**
- **Human Right Act (1998)**

Emerging technologies are examined for educational benefit and a risk assessment is carried out before use in school is allowed.

Digital and video images (including cameras and iPads)

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff and pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. The school will inform and educate users about these risks to reduce the likelihood of the potential for harm.

- Consent is required under the Data Protection Act 2018
- Images must not be used for anything other than the agreed purposes, unless additional consent is obtained (images are considered personal data under the Data Protection Act 2018)
- All images are to be stored and disposed of in line with the Data Protection Act 2018
- If images are to be stored for a short period of time, they must be on a password protected computer storage device
- Digital images are only taken using approved technologies ie flip cams, web cams, iPads and cameras – Personal mobile phones should **never** be used to take images or videos of pupils
- iPad minis used to capture evidence for EYFS profiling and assessment must be pass code protected
- The purpose and context for any proposed images should always be considered to decide whether a photograph or video are the most appropriate method of recording the information
- Photographic permissions/consent **must** be obtained from parents/carers with parental responsibility at least annually
- Photographs must be appropriately disposed of should they no longer be required.
- Where group photographs of children are to be taken, written permission must be obtained from all parents/carers, who have the right to refuse.
- The purpose of taking images is to be clearly explained.
- Parents reserve the right to withdraw consent at any time
- Consent to the use of images applies to adults as well as children
- A child's full name should not appear alongside their photographs, particularly if the images

could be viewed by the general public

Mobile Phones

- Under no circumstances are images, videos or audio recordings to be made using personal mobile phones
- To minimize any risks, all personal mobiles must not be used during lessons.
- Vistors, including other professionals and contactors must be made aware that they are not to use their phone where children are present (this may be via AUA where appropriate)
- Staff are advised to provide their work place contact number to their family members/own children's schools/settings for use in the event of an emergency
- The sending of abusive or inappropriate text messages is forbidden.
- The school will not be held responsible for any loss or damage of personal mobile phones
- Children are only allowed to bring mobile phones into school under exceptional circumstances, where permission has been sought. These phones must be handed in to the school office and remain switched off during the school day.

Use of a professional photographer

- Only a reputable photographer who can provide evidence of authenticity should be used. Their photographic identity should be checked on arrival.
- Photographers should be viewed as visitors, therefore appropriate supervisions should be in place at all times to ensure no unsupervised access to children.
- Photographers should be asked to sign an agreement to ensure that they comply with Data Protection requirements and AUA.
- Photographers must agree that images will only be used for the agreed specified purpose and not disclosed to any third person.

Parents/Carers

- The use of any photographic equipment by parents or visitors must be with the consent of the Principal
- The Principal has the authority to challenge anyone using photographic equipment without prior consent
- Parents and carers are not covered by the Data Protection Act if they take photgraphs or make a video recording for their own private use

Closed Circuit Television (CCTV)

- Images of people are covered by the Data Protection Act and therefore applies to CCTV
- All areas covered by CCTV are sign posted and notifications are displayed
- Data Protection and information guidelines are to be followed at all times (please refer to ICO publication 'CCTV code of practice.' Revised edition 2008.)

COMPUTER & NETWORK SECURITY

The Vice principal is the whole school systems manager. At Longford we are registered with the data protection agency and any data files on the administrative system is password protected. Personal

data will be recorded, processed, transferred and made available according to the Data Protection Act 2018. The school has adopted the county policy on ICT security (appendix 5).

The school will be responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented

- School ICT systems will be managed in ways that ensure that the school meets the e-safety technical requirements outlined in the LA Security Policy (appendix 5) and AUAs (appendices 6&7) and any relevant LA guidance
- There will be regular reviews and audits of the safety and security of school ICT systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school ICT systems. Details of the access rights available to groups of users will be recorded by the Network Manager and will be reviewed annually.
- All staff users will be provided with a username and password. Pupil users will be provided with an anonymous username.
- The administrator passwords for the school ICT system, used by the Network manager must also be available to the Principal and kept in a secure place.
- Users will be made responsible for the security of their username and password, and must not allow other users to access the systems using their log on details
- The school maintains and supports the managed filtering service provided by the LA
- In the event of the Network Manager needing to switch off the filtering for any reason, or for any user, this must be logged
- Any filtering issues should be reported immediately to LT (Learning Technologies) at entrust.
- Requests from staff for sites to be removed from the filtered list will be considered by the Network Manager and the Principal.
- School ICT technical staff regularly monitor and record the activity of users on the school ICT systems
- Users must report any actual/potential e-safety incident to the Network Manager.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc from accidental or malicious attempts which might threaten the security of the school systems and data.
- Guest users such as trainee teachers, visitors etc must read and sign the e-safety code of conduct and AUP before using the school system.
- Each piece of software that is installed onto the system must have a valid licence. These are held by the Vice principal, along with master disks. No software, other than that we are licensed for may be installed.
- No disks from outside sources may be bought into school for intallation. However, USB pen drives and external hard drives may be used to access material. The whole system is protected by Symantic antivirus. Any attempt to hack the system or introduce a virus is a dismissable offence.
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Misuse

Some internet activity eg accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other ICT systems. Other activities eg Cyber-bullying would be banned and could lead to criminal prosecution. It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

If members of staff suspect that misuse might have taken place, but that the misuse is not illegal it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, according to AUA, and that members of the school community are aware that incidents have 1been dealt with. Incidents of misuse, both inside and outside school, will be logged and dealt with in line with the behaviour policy and normal disciplinary procedures.

This policy should be read in conjunction with:

- ICT Policy & appendices
- Safeguarding Policy
- PSHE Policy
- Behaviour Policy
- Anti-bullying policy
- EYFS Policy

Appendices

1. Pupil acceptable use agreements - code of conduct & photographic/video consent form (KS1 & KS2)
2. Parental code of conduct & photographic/video consent form (EYFS)
3. Staff acceptable use agreements - code of conduct
4. Responding to incidents of misuse
5. ICT Security Policy
6. Code Of Practice For Employees in the use of Social Networking Sites and Electronic Media