November | 21

Amadeus
Primary Academies Trust
Limitless Learning Together

Holy Trinity Lamorbey CE Primary School Online Safety Policy

Table of Contents

Introduction and Overview

The purpose of this policy is to:

- set out the key principles expected of all members of the school community at Holy Trinity Lamorbey CE Primary School (HTL) with respect to the use of ICT-based technologies.
- safeguard and protect the children and staff of HTL.
- assist school staff working with children to work safely and responsibly with the internet and other communication technologies and to monitor their own standards and practice.
- set clear expectations of behaviour and/or codes of practice relevant to responsible use of the internet for educational, personal or recreational use.
- draw awareness to online abuse such as cyberbullying which are cross referenced with other school policies and documentation.
- ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- minimise the risk of misplaced or malicious allegations made against adults who work with students.

ICT in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment. Information and Communications Technology (ICT) covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites;
- Learning Platforms and Virtual Learning Environments;
- Email and Instant Messaging;
- Chat Rooms and Social Networking (Facebook, Whats App, Skype etc);
- Blogs and Wikis;
- Podcasting;
- Video Broadcasting;
- Music Downloading;
- Gaming;
- Online gaming;
- Mobile/ Smart phones with text, video and/ or web functionality;
- Other mobile devices with web functionality (e.g. tablets).

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies.

At HTL, we understand the responsibility to educate our pupils on e-Safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom. Both this policy and the acceptable use agreement (for all staff, governors, visitors and pupils) include both fixed and mobile internet; technologies provided by the school(such as PCs, laptops, personal digital assistants (PDAs), tablets, webcams, whiteboards, voting systems, digital video equipment, etc); and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobile phones, camera phones, PDAs and portable media players, etc).

Expected Conduct

In our school, all users:

- are responsible for using the school ICT systems in accordance with the relevant acceptable use policy which they will be expected to sign before being given access to school systems (at KS1 it would be expected that parents/carers would sign on behalf of the pupils)
- need to understand the importance of misuse or access to inappropriate materials and are aware of the consequences
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- should understand the importance of adopting good e-Safety practice when using digital technologies out of school and realise that the school's online safety policy covers their actions out of school, if related to their membership of the school
- will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking/use of images and on cyber-bullying

Staff

- are responsible for reading the school's online safety policy and using the school ICT systems accordingly, including the use of mobile phones, and hand held devices.

Students/Pupils

- should have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations

Parents/Carers

- should provide consent for pupils to use the Internet, as well as other technologies, as part of the acceptable use agreement form at time of their child's entry to the school
- should know and understand what the 'rules of appropriate use' are and what sanctions result from misuse

Managing the ICT Infrastructure Internet access, security (virus protection) and filtering

Our school:

- Has the educational filtered secure broadband connectivity through the LGfL and so connects to the 'private' National Education Network;
- Uses the LGfL filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature, etc. All changes to the filtering policy is logged and only available to staff with the approved 'web filtering management' status Via the Atomwide helpdesk;
- Uses USO user-level filtering where relevant, thereby closing down or opening up options

appropriate to the age/stage of the students;

- Ensures healthy network through use of Sophos anti-virus software (from LGfL) etc and network set-up so staff and pupils cannot download executable files;
- Uses DfE, LA or LGfL approved systems such as S2S, USO FX, secured email to send personal data over the Internet and uses encrypted devices or secure remote access where staff need to access personal level data off-site;
- LGFL Blocks all chat rooms and social networking sites except those that are part of an educational network or approved Learning Platform;
- Only unblocks other external social networking sites for specific purposes/Internet Literacy lessons;
- Has blocked pupil access to music download or shopping sites – except those approved for educational purposes at a regional or national level, such as Audio Network;
- Works in partnership with the LGfL to ensure any concerns about the system are communicated so that systems remain robust and protect students;
- Is vigilant in its supervision of pupils' use at all times, as far as is reasonable, and uses common-sense strategies in learning resource areas where older pupils have more flexible access;
- Ensures all staff and students have signed an acceptable use agreement form and understands that they must report any concerns;
- Ensures pupils only publish within an appropriately secure environment: the school's learning environment/ the London LEARNING PLATFORM/ LGfL secure platforms such as J2Bloggy, etc
- Requires staff to preview websites before use (where not previously viewed or cached) and encourages use of the school's Learning Platform as a key way to direct students to age/subject appropriate web sites; Plans the curriculum context for Internet use to match pupils' ability, using child-friendly search engines where more open Internet searching is required; eg yahoo for kids or ask for kids , Google Safe Search;
- Never allows/is vigilant when conducting 'raw' image search with pupils eg Google image search;
- Informs all users that Internet use is monitored;
- Informs staff and students that that they must report any failure of the filtering systems directly to the (system administrator/teacher/person responsible for URL filtering). Our system administrator(s) logs or escalates as appropriate to the technical service provider or Atomwide Helpdesk as necessary;
- Makes clear all users know and understand what the 'rules of appropriate use' are and what sanctions result from misuse –through staff meetings and teaching programme;
- Provides advice and information on reporting offensive materials, abuse/bullying etc available for pupils, staff and parents;
- Immediately refers any material we suspect is illegal to the appropriate authorities (Police and the LA).

Network Management

Our school:

- (uses individual) staff individual log-ins and pupil year group log-ins, audited log-ins for all users: the London USO system;
- uses guest accounts occasionally for external or short-term visitors for temporary access to appropriate services; occasional guests do not have access to the public drive
- uses teacher 'remote' management control tools for controlling workstations/viewing users/setting-up applications and Internet websites, where useful;

- has additional local network auditing software installed;
- ensures the Systems Administrator/Network Manager is up-to-date with LGfL services and policies/requires the Technical Support Provider to be up-to-date with LGfL services and policies;
- storage of all data within the school will conform to the UK data protection requirements. Pupils and Staff using mobile technology, where storage of data is online, will conform to the EU data protection directive where storage is hosted within the EU.

To ensure the network is used safely, our school:

- ensures staff read and sign that they have understood the school's online safety policy. Following this, they are set-up with Internet, email access and network access. Online access to service is through a unique, audited username and password. We also provide a different/use the same username and password for access to our school's network; staff individual log-ins and pupil year group login passwords changed annually
- staff access to the schools' management information system is controlled through a separate password for data security purposes; Sims system has restricted access for only the Office Staff and Senior Management only. Access granted by Sims team and agreed with the Office Manager and HeadTeacher
- we provide pupils with a class network log-in username. From Year R they are also expected to use a class password;
- we use the London Grid for Learning's Unified Sign-On (USO) system for username and passwords;
- makes clear that no one should log on as another user and makes clear that pupils should never be allowed to log-on or use teacher and staff logins as these have far less security restrictions and inappropriate use could damage files or the network;
- has set-up the network with a shared work area for pupils and one for staff. Staff and pupils are shown how to save work and access work from these areas;
- requires all users to always log off when they have finished working or are leaving the computer unattended;
- where a user finds a logged-on machine, we require them to always log-off and then log-on again as themselves (users needing access to secure data Target Tracker & Sims); • requests that teachers and pupils do not switch the computers off during the day unless they are unlikely to be used again that day or have completely crashed. We request that they DO switch the computers off at the end of the day;
- •network users can download executable files/programs but cannot run these programs unless Teacher power user rights;
- LGFL have blocked access to music/media download or shopping sites – except those approved for educational purposes;
- makes clear that staff are responsible for ensuring that all equipment that goes home has the anti-virus and spyware software maintained up-to-date and the school provides them with a solution to do so;
- makes clear that staff are responsible for ensuring that any computer or laptop loaned to them by the school is used solely to support their professional responsibilities and that they notify the school of any "significant personal use" as defined by HM Revenue & Customs.
- makes clear that staff accessing LA systems do so in accordance with any Corporate policies e.g. Borough email or Intranet; finance system, Personnel system etc;
- maintains equipment to ensure Health and Safety is followed eg projector filters cleaned by site manager/TA; equipment installed and checked by approved Suppliers/LA electrical engineers;

- has integrated curriculum and administration networks, but access to the Management Information System is set-up so as to ensure staff users can only access modules related to their role eg teachers access report writing module; SEN coordinator - SEN data as setup by Atomwide helpdesk;
- ensures that access to the school's network resources from remote locations by staff is restricted and access is only through school/LA approved systems eg teachers access their area/a staff shared area for planning documentation via a VPN solution / RAv3 system; (Rav3 access for administrator and Head Teachers only);
- does not allow any outside Agencies to access our network remotely except where there is a clear professional need and then access is restricted and is only through approved systems eg technical support or MIS Support, our Education Welfare Officers accessing attendance data on specific children, parents using a secure portal to access information on their child;
- provides pupils and staff with access to content and resources through the approved LGFL Learning Platform which staff and pupils access using their username and password (their USO username and password);
- makes clear responsibilities for the daily back up of MIS and finance systems and other important files;
- has a clear disaster recovery system in place for critical data that includes a secure, remote back-up of critical data, that complies with external Audit's requirements;
- uses the DfE secure s2s website for all CTF files sent to other schools as set up by the Sims team;
- ensures that all pupil level data or personal data sent over the Internet is encrypted or only sent within the approved secure system in our LA or through USO secure file exchange (USO FX);
- follows ISP advice on Local Area and Wide Area security matters and firewalls and routers have been configured to prevent unauthorised use of our network;
- our wireless network has been secured to industry standard Enterprise security level /appropriate standards suitable for educational use;
- •all computer equipment is installed professionally and meets health and safety standards;
- projectors are maintained so that the quality of presentation remains high;
- reviews the school ICT systems regularly with regard to health and safety and security.

Online Safety and the PREVENT strategy

Our policy and practice ensures that:

- Children are safe from terrorist and extremist material when accessing the internet in school, including by establishing appropriate levels of filtering (through appropriate school level and/or external (lgfl) filtering.
- We ensure pupils cannot access dangerous content, or be contacted online by extremist groups.
- General internet safety is embedded in our school's computing curriculum.
- Every teacher is aware of the risks posed by the online activity of extremist and terrorist groups.

Passwords Policy

- This school makes it clear that staff and pupils must always keep their password private. They must not share it with others and must not leave it where others can find.
- All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password private.
- We require staff to use a STRONG password for access into our MIS system.

E-mail

This school:

- provides staff with two email accounts for their professional use, London Staffmail/LA email and Google Mail through the HTL account.
- makes clear personal email should be through a separate account;
- does not publish personal e-mail addresses of pupils or staff on the school website. We use anonymous or group e-mail addresses, eg info@schoolname.la.sch.uk / head@schoolname.la.sch.uk / or class e-mail addresses (with one or more staff having access to an aliased/shared mailboxfor a class) for communication with the wider public.
- will contact the Police if one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law;
- will ensure that email accounts are maintained and up to date;
- reports messages relating to or in support of illegal activities to the relevant Authority and if necessary to the Police;
- Knows that spam, phishing and virus attachments can make emails dangerous. We use a number of LGfL provided technologies to help protect users and systems in the school, including desktop anti-virus product Sophos, plus direct email filtering for viruses, Trojans, pornography, phishing and inappropriate language. Finally, and in support of these, LGfL WebScreen2 filtering monitors and protects our internet access to the World Wide Web.

Pupils:

- Pupils are introduced to email as part of the Computing Scheme of Work.
- Pupils sign the school agreement form to say they have read and understood the online safety rules, including e-mail and we explain how any inappropriate use will be dealt with.

Staff:

- Staff can only use the LA, LGfL or HTL Google Mail e-mail systems on the school system
- Staff use a ‘closed’ LA e-mail system which is used for LA communications and some ‘LA approved’ transfers of information
- Never use e-mail to transfer staff or pupil personal data. We use secure, LA/DfE approved systems. These include: S2S (for school to school transfer); Collect; USOFX, Atomwide and EGRESS; Staff know that e-mail sent to an external organisation must be written carefully, (and may require authorisation), in the same way as a letter written on school headed paper. That it should follow the school ‘house-style’:
- •the sending of multiple or large attachments should be limited, and may also be restricted by the provider of the service being used;
- the sending of chain letters is not permitted;
- embedding adverts is not allowed.

- All staff sign our LA / school Agreement Form AUP to say they have read and understood the e-safety rules, including e-mail and we explain how any inappropriate use will be dealt with.

Social Networking and Staff

- Teachers are instructed not to run social network spaces for student use on a personal basis or to open up their own spaces to their students, but to use the schools' preferred system for such communications.
- School staff will ensure that in private use:
- No reference should be made in social media to students/pupils, parents/carers or school staff;
- They do not engage in online discussion on personal matters relating to members of the school community;
- Personal opinions should not be attributed to the school/academy or local authority;
- Security settings on personal social media profiles are regularly checked to minimize risk of loss of personal information.

Social Networking and Pupils

- Through assemblies, PSHE, online safety week activities and informing parents and pupils of new concerns raised by new media / app developments, we ensure that children and their carers are aware and able to make informed decision around social media, report their concerns (including peer on peer abuse, sexting and harassment). This is further supported by Child Protection policy, our Mobile Phone policy and half termly safety elements to each Computing unit.

Equipment and Digital Content Personal mobile phones and mobile devices (iPads)

- Mobile phones or iPads brought into school are entirely at the staff member, student's & parents' or visitors own risk. The School accepts no responsibility for the loss, theft or damage of any phone or hand held device brought into school.
- Student mobile phones which are brought into school must be turned off (not placed on silent) and stored in the school office until collection at the end of the day.
- The recording, taking and sharing of images, video and audio on any mobile phone or personal iPad is to be avoided; except where it has been explicitly agreed otherwise by the Head of School. Such authorised use is to be monitored and recorded. All use is to be open to scrutiny and the Head of School is to be able to withdraw or restrict authorisation for use at any time if it is to be deemed necessary.
- The School reserves the right to search the content of any mobile or handheld device on the school premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence or bullying. Staff mobiles or hand held devices may be searched at any time as part of routine monitoring.
- Where parents or students need to contact each other during the school day, they should do so only through the School's telephone. Staff may use their phones during break times.
- Mobile phones and personally-owned devices will not be used in any way during lessons or formal school time. They should be switched off or silent at all times.

Staff Use of Personal Devices

- Staff should not use personally-owned devices, such as mobile phones or cameras, to take photos or videos of students and will only use work-provided equipment for this purpose.
- If a member of staff breaches the school policy then disciplinary action may be taken. • In an emergency for contacting students or parents a staff member should use their own device and hide (by inputting 141) their own mobile number for confidentiality purposes.

Digital Images and Video

In this school:

- We gain parental/carer permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter/son joins the school;
- We do include the full names of pupils in the credits of any published school produced video materials/DVDs;
- Staff sign the school's acceptable use policy and this includes a clause on the use of mobile phones/personal equipment for taking pictures of pupils;
- If specific pupil photos (not group photos) are used on the school website, in the prospectus or in other high profile publications the school will obtain individual parental or pupil permission for its long-term use
- The school blocks/filters access to social networking sites or news groups unless there is a specific approved educational purpose;
- Pupils are taught about how images can be manipulated in their e-Safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children as part of their ICT scheme of work;
- Pupils are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.
- Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identify of others and their location, such as house number, street name or school. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse. School Website
- The Head Teacher takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained;
- Uploading of information is restricted to our website authorisers
- The school website complies with the statutory DfE guidelines for publications;
- Most material is the school's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status;
- The point of contact on the website is the school address, telephone number and we use a general e-mail contact address, e.g. admin@schooladdress. Home information or individual e-mail identities will not be published;
- Photographs published on the web do not have full names attached;
- We do not use pupils' names when saving images in the file names or in the tags when publishing

to the school website;

- We do not use embedded geo-data in respect of stored images;
- We expect teachers using school approved blogs or wikis to password protect them and run from the school website.