The Livity School
E-Safety Policy

Contents

Appendices:

1. Introduction and Overview

Rationale
The purpose of this policy is to:

- set out the key principles expected of all members of the school community at The Livity School with respect to the use of ICT-based technologies.
- safeguard and protect the children and staff of The Livity School
- 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.
- have clear structures to deal with any online abuse
- 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.

Areas of risk can be summarised as follows:

All areas are of concern, though for our school not all aspects are necessarily the same risk for The Livity School pupils due to their severe disability. However for those pupils able to access the internet or use hand held devices, the risk could be greater due to their vulnerability.

Content however these are filtered by LGFL

- exposure to inappropriate content, including online pornography, exposure to violence and inappropriate language
- repeated viewing of content which is not overtly damaging, but is inappropriate for pupils to emulate
- content validation: how to check authenticity and accuracy of online content
- lifestyle websites, for example pro-anorexia/self-harm/suicide sites
- hate sites

Contact

- grooming
- cyber-bullying in all forms
- sexting (sending and receiving of personally intimate images) also referred to as SGII (self generated indecent images)

Conduct

- privacy issues, including disclosure of personal information
- identity theft (including 'frape' (hacking Facebook profiles)) and sharing password
- digital footprint and online reputation

- health and well-being (amount of time spent online (internet or gaming))
- copyright (little care or consideration for intellectual property and ownership – such as music and film)

(Ref Ofsted 2013)

Scope

This policy applies to all members of The Livity School community (including staff, students / pupils, volunteers, visiting professionals, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of The Livity School

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the *school* site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school / academy. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data (see appendix for template policy). In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

The Livity School will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school.

Role	Key Responsibilities
Headteacher	• To take overall responsibility for e-Safety provision • To take overall responsibility for data and data security (SIRO) • To ensure the school uses an approved, filtered Internet Service, which complies with current statutory requirements eg LGfL • To be responsible for ensuring that staff receive suitable training to carry out their e-safety roles and to train other colleagues, as relevant • To be aware of procedures to be followed in the event of a serious e-Safety incident. • To receive regular monitoring reports from the E-Safety Co-ordinator / Officer • To ensure that there is a system in place to monitor and support staff who carry out internal e-safety procedures(e.g. network manager)

Role	Key Responsibilities

e-Safety Co-ordinator / Designated Child Protection Lead	• takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents
	• promotes an awareness and commitment to e-safeguarding throughout the school community
	• ensures that e-safety education is embedded across the curriculum
	• liaises with school ICT technical staff
	• To communicate regularly with SLT and the designated e-Safety Governor / committee to discuss current issues, review incident logs and filtering / change control logs
	• To ensure that all staff are aware of the procedures that need to be followed in the event of an e-Safety incident
	• To ensure that an e-Safety incident log is kept up to date
	• facilitates training and advice for all staff
	• liaises with the Local Authority and relevant agencies
	• Is regularly updated in e-safety issues and legislation, 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 and use of social media

Governors / E-safety governor	• To ensure that the school follows all current e-Safety advice to keep the children and staff safe
	• To approve the E-Safety Policy and review the effectiveness of the policy. This will be carried out by the Governors / Governors Sub Committee receiving regular information about e-safety incidents and monitoring reports. A member of the Governing Body has taken on the role of E-Safety Governor
	• To support the school in encouraging parents and the wider community to become engaged in e-safety activities
	• The role of the E-Safety Governor will include:
	  • regular review with the E-Safety Co-ordinator / Officer (including
	  e-safety incident logs, filtering / change control logs)

Computing Curriculum Leader	• To oversee the delivery of the e-safety element of the Computing curriculum • To liaise with the e-safety coordinator regularly
Network Manager/technician	• To report any e-Safety related issues that arises, to the e-Safety coordinator. • To ensure that users may only access the school's networks through an authorised and properly enforced password protection policy, in which passwords are regularly changed • To ensure that provision exists for misuse detection and malicious attack e.g. keeping virus protection up to date RM constantly monitor system for attacks and viruses. LGFL also scan the schools ports and notify school if they suspect

Role	Key Responsibilities
	viruses. • To ensure the security of the school ICT system • To ensure that access controls / encryption exist to protect personal and sensitive information held on school-owned devices • the school's policy on web filtering is applied and updated on a regular basis LGFL filter to the agreed Lambeth Standard • LGfL is informed of issues relating to the filtering applied by the Grid • that he / she keeps up to date with the school's e-safety policy and 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 / remote access / email* is regularly monitored in order that any misuse / attempted misuse can be reported to the *E-Safety Co-ordinator / Officer /Headteacher for investigation / action / sanction* • To ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster. • To keep up-to-date documentation of the school's e-security and technical procedures
Data Manager	• To ensure that all data held on pupils on the school office machines have appropriate access controls in place Office staff all have unique user names and passwords
LGfL Nominated contact(s)	• To ensure all LGfL services are managed on behalf of the school including maintaining the LGfL USO database of access accounts Technician manages our USO data base
Teachers	• To embed e-safety issues in all aspects of the curriculum and other school activities • To supervise and guide pupils carefully when engaged in learning activities involving online technology (including, extra curricular and extended school activities if relevant) • To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws
All staff	• To read, understand and help promote the school's e-Safety policies and guidance • To read, understand, sign and adhere to the school staff Acceptable Use Agreement / Policy • To be aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices • To report any suspected misuse or problem to the e-Safety coordinator • To maintain an awareness of current e-Safety issues and guidance e.g. through CPD • To model safe, responsible and professional behaviours in their own use of technology

Role	Key Responsibilities
	• To ensure that any digital communications with pupils and parents should be on a professional level and only through school based systems, never through personal mechanisms, e.g. email, text, mobile phones etc.
Pupils	• Parents to read, understand, sign and adhere to the Pupil Acceptable Use Policy (on behalf of the pupils) • To follow and where possible understand the importance of adopting good e-safety practice when using digital technologies
Parent Liasion Officer	• Educating Parents and raising awareness as instructed by Head?
Parents/carers	• to support the school in promoting e-safety and endorse the Parents' Acceptable Use Agreement which includes the pupils' use of the internet and the school's use of photographic and video images • to read, understand and promote the school Pupil Acceptable Use Agreement with their children • to access the school website and any other school online information in accordance with the relevant school Acceptable Use Agreement. • to consult with the school if they have any concerns about their children's use of technology
External groups	• Any external individual / organisation will sign an Acceptable Use Policy prior to using any equipment or the internet within school

Communication:
How the policy will be communicated to staff/pupils/community in the following ways:

- Policy to be posted on the school website and held in class handbooks.
- Policy to be part of school induction pack for new staff
- Acceptable use agreements to be issued to whole school community, usually on entry to the school
- Acceptable use agreements to be held in personnel files

Handling complaints:

- The school will take all reasonable precautions to ensure e-Safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the school nor the Local Authority can accept liability for material accessed, or any consequences of Internet access.

- Staff are given information about infringements in use and possible sanctions. Sanctions available include:
- removal of Internet or computer access for a period, [which could referral to LA / Police.

- Our e-Safety Coordinator acts as first point of contact for any complaint. Any complaint about staff misuse is referred to the Headteacher.

- Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with school / LA child protection procedures.

Review and Monitoring

The e-safety policy is referenced from within other school policies: ICT and Computing policy, Child Protection policy, Anti-Bullying policy and in the School Development Plan, Behaviour policy, Personal, Social and Health Education and for Citizenship policies .

- The school has an e-safety coordinator who will be responsible for document ownership, review and updates.
- The e-safety policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the school
- The e-safety policy has been written by the school e-safety Coordinator and is current and appropriate for its intended audience and purpose.
- There is widespread ownership of the policy and it has been agreed by the SLT and approved by Governors and other stakeholders such as the PTA. All amendments to the school eSafeguarding policy will be discussed in detail with all members of teaching staff.

Version Control

As part of the maintenance involved with ensuring your e-safety policy is updated, revisions will be made to the document. It is important that the document owner ensures the document contains the following information and that all revisions are stored centrally for audit purposes.

Title	The Livity School e-safety policy
Version	1.0
Date	DD/MM/YYYY
Author	e-safety coordinator
Approved by head teacher	
Approved by Governing Body	
Next Review Date	

Modification History

Version	Date	Description	Revision Author
0.1		Initial draft	e-safety coordinator

2. Education and Curriculum

Pupil e-Safety curriculum

This school

- Delegates the responsibility for the e-safety of it's pupils to the staff working directly with the pupils. Few pupils are able to understand the dangers of accessing specific sites and all pupils require supervision whilst using the internet and other technologies. Many pupils require adult support to access technology and those who are able to access it independently have limited understanding of the dangers it could present.
- will model safe practice and also teach pupils where appropriate about e-safety. As part of the ICT curriculum / and PSHE curriculum, for example
    - to understand acceptable behaviour when using an online environment / email, i.e. be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private;
    - to understand why on-line 'friends' may not be who they say they are and to understand why they should be careful in online environments;
    - to understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos
    - to know not to download any files – such as music files - without permission;
    - to know how to report any abuse; and how to to seek help if they experience problems when using the internet and related technologies, i.e. parent or carer, teacher or trusted staff member.
- Plans internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.
- Ensures staff will model safe and responsible behaviour in their own use of technology during lessons.
- Ensures that when copying materials from the web, staff understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright / intellectual property rights;
- Ensures that staff and (pupils where appropriate) understand the issues around aspects of the commercial use of the Internet, as age appropriate. This may include, risks in pop-ups; buying on-line; on-line gaming / gambling;

Staff and governor training

This school

- Ensures staff know how to send or receive sensitive and personal data and understand the requirement to encrypt data where the sensitivity requires data protection;
- Makes regular training available to staff on e-safety issues and the school's e-safety education program
- Provides ,as part of the induction process, all new staff [including those on university/college placement and work experience] with information and guidance on the eSafeguarding policy and the school's Acceptable Use Policies.

Parent awareness and training

This school

- runs a rolling programme of advice, guidance and training for parents, including:
- Introduction of the Acceptable Use Agreements to new parents, to ensure that principles of e-safe behaviour are made clear
- Information leaflets; in school newsletters; on the school web site;
- demonstrations, practical sessions held at school;
- suggestions for safe Internet use at home;
- provision of information about national support sites for parents.

3. Expected Conduct and Incident management

Expected conduct

In this 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. (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 E-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 e-safety policy and using the school ICT systems accordingly, including the use of mobile phones, and hand held devices.

Parents/Carers

- should provide consent for pupils to use the Internet, as well as other technologies, as part of the e-safety 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

Incident Management

In this school:

- there is strict monitoring and application of the e-safety policy and a differentiated and appropriate range of sanctions, though the attitudes and behaviour of users are generally positive and there is rarely need to apply sanctions

- all members and its wider community are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the school's escalation processes.
- support is actively sought from other agencies as needed (eg the local authority and regional broadband grid, UK Safer Internet Centre helpline) in dealing with e-safety issues
- monitoring and reporting of e safety incidents takes place and contribute to developments in policy and practice in e-safety within the school. The records are reviewed/audited and reported to the school's senior leaders, Governors /the LA / LSCB
- parents / carers are specifically informed of e-safety incidents involving young people for whom they are responsible.
- We will contact the Police if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law

4. Managing the ICT infrastructure

- **Internet access, security (virus protection) and filtering**

This school:

- Has the educational filtered secure broadband connectivity through the LGfL and so connects to the 'private' National Education Network;
- Uses the LGfL Net Sweeper 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;
- On request we are able to block any sites that we feel are inappropriate
- Ensures network healthy through use of Symantec anti-virus software (from RM) etc and network is set-up so staff can down load executable files but 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 were staff need to access personal level data off-site;
- Blocks all Chat rooms and social networking sites
- 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.
- Ensures all staff and parents have signed an acceptable use agreement form and understands that they must report any concerns;

- 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, where appropriate using child-friendly search engines where more open Internet searching is required; eg yahoo for kids or ask for kids , Google Safe Search , Espresso
- Never allows 'raw' image search with pupils e.g. Google image search;
- Informs all users that Internet use is monitored;
- Informs staff 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 LGfL 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 (user access, backup)**
  This school
  - Uses individual, audited log-ins for all adult users currently pupils have collective class logins which the class staff use to log in pupils
  - Uses guest accounts occasionally for external or short term visitors for temporary access to appropriate services
  - *Uses teacher 'remote' management control tools for controlling workstations / viewing users / setting-up applications and Internet web sites, where useful; RAV3 System.*
  - 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

To ensure the network is used safely, this school:

- Ensures staff read and sign that they have understood the school's e-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 access to the schools' management information system is controlled through a separate password for data security purposes;
- We provide classes with an individual network log-in username.

- We use the London Grid for Learning's Unified Sign-On (USO) system for email 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 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 are timed out after 10 mins and have to re-enter their username and password to re-enter the network.];
- 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 and we also automatically switch off all computers at 8 o'clock to save energy;
- Has set-up the network so that pupils cannot download executable files / programmes;
- Has blocked access to music/media download or shopping sites on the main computers used by pupils – except those approved for educational purposes
- Scans all mobile equipment with anti-virus / spyware before it is connected to the network;
- 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;
  e.g. 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
- 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:
  e.g. teachers access their area / a staff shared area for planning documentation via a VPN solution / RAv3 system;

- 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;
  e.g. technical support or MIS Support, Education Welfare Officers accessing attendance data on specific children,
- 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 our broadband network for our CCTV system and have had set-up by approved partners;
- Uses the DfE secure s2s website for all CTF files sent to other schools;
- 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.

Passwords policy

- This school makes it clear that staff and pupils must always keep their password private, 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 <STRONG passwords for access into our MIS system>.
- We require staff to change their passwords into the MIS, LGfL USO admin site, twice a year.

E-mail

This school

- Provides staff with an email account for their professional use, *London Staffmail / LA email* and makes clear personal email should be through a separate account;
- Will Provide *highly restricted (Safe mail) / simulated environments for e-mail with pupils* should this be appropriate e.g. Uses Londonmail with students as this has email content control

- Does not publish personal e-mail addresses of pupils or staff on the school website. We use anonymous or group e-mail addresses
- 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 e mails dangerous. We use a number of LGfL-provided technologies to help protect users and systems in the school, including desktop anti-virus product Symantec, 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: If appropriate we will

- Introduce pupils to use of e-mail as part of the ICT/Computing scheme of work.
- LGfL LondonMail will be used with pupils and locked down where appropriate using LGfL SafeMail rules.
- Pupils' LGfL LondonMail e-mail accounts are intentionally 'anonymised' for their protection..
- Pupils can only receive external mail from, and send external mail to, addresses if the SafeMail rules have been set to allow this.
- Pupils are taught about the safety and 'netiquette' of using e-mail both in school and at home i.e. they are taught:
    - not to give out their e-mail address unless it is part of a school managed project or to someone they know and trust and is approved by their teacher or parent/carer;
    - that an e-mail is a form of publishing where the message should be clear, short and concise;
    - that any e-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper;
    - they must not reveal private details of themselves or others in e-mail, such as address, telephone number, etc;
    - to 'Stop and Think Before They Click' and not open attachments unless sure the source is safe;
    - that they should think carefully before sending any attachments;
    - embedding adverts is not allowed;
    - that they must immediately tell a teacher / responsible adult if they receive an e-mail which makes them feel uncomfortable, is offensive or bullying in nature;
    - not to respond to malicious or threatening messages;
    - not to delete malicious of threatening e-mails, but to keep them as evidence of bullying;

- not to arrange to meet anyone they meet through e-mail without having discussed with an adult and taking a responsible adult with them;
- that forwarding 'chain' e-mail letters is not permitted.

- Parents of Pupils sign the school Agreement Form 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.

Staff:

- Staff can only use the LA or LGfL e mail systems on the school system
- Staff only use LA or LGfL e-mail systems for professional purposes
- Access in school to external personal e mail accounts may be blocked
- Staff use a 'closed' LA email system which is used for LA communications and some 'LA approved' transfers of information ;
- Never use email to transfer staff or pupil personal data. We use secure, LA / DfE approved systems. These include: S2S (for school to school transfer); Collect; USO-FX*, named LA system;*
- 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.

School website

- The Headteacher 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 web site 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 web site is the school address, telephone number and we use a general email contact address, admin@thelivity.lambeth.sch.uk 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 geodata in respect of stored images

Social networking

- 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.

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 minimise risk of loss of personal information.

Video Conferencing

This school

- Only uses the LGfL / Janet supported services for video conferencing activity;
- Only uses approved or checked webcam sites;

CCTV

- We have CCTV in parts of the school as part of our site surveillance for staff and student safety. We will not reveal any recordings (*retained by the Support Provider for 28 days*), without permission except where disclosed to the Police as part of a criminal investigation.
- We use specialist lesson recording equipment on occasions as a tool to share best teaching practice. We do not reveal any such recordings outside of the staff and will not use for any other purposes.

5. Data security: Management Information System access and Data transfer

Strategic and operational practices

At this school:

- The Head Teacher is the Senior Information Risk Officer (SIRO).
- We ensure staff know who to report any incidents where data protection may have been compromised.
- All staff are DBS checked and records are held in one central record in SIMS /speadsheet.

  We ensure ALL the following school stakeholders sign an Acceptable Use Agreement form. We have a system so we know who has signed.

  - staff,
  - governors,
  - parents
  - visiting professionals who have access to the school network

This makes clear staffs' responsibilities with regard to data security, passwords and access.

- We follow LA guidelines for the transfer of any data, such as MIS data or reports of children, to professionals working in the Local Authority or their partners in Children's Services / Family Services, Health, Welfare and Social Services.
- We require that any Protect and Restricted material must be encrypted if the material is to be removed from the school and limit such data removal. / We have an approved remote access solution so staff can access sensitive and other data from home, without need to take data home.
- We ask staff to undertaken at least annual house-keeping to review, remove and destroy any digital materials and documents which need no longer be stored.

Technical Solutions

- Staff have <secure area(s) on the network to store sensitive documents or photographs>.
- We require staff to log-out of systems when leaving their computer, but also enforce lock-out after 10 mins idle time.
- We use <encrypted flash drives> if any member of staff has to take any sensitive information off site.
- We use the DfE S2S site to securely transfer CTF pupil data files to other schools.
- We use < RAv3 / VPN solution> with its 2-factor authentication for remote access into our systems.
- We use <LGfL's USO FX> to transfer other data to schools in London, such as references, reports of children.
- We use the LGfL secure data transfer system, USOAutoUpdate, for creation of online user accounts for access to broadband services and the London content
- We store any Protect and Restricted written material in lockable storage cabinets or in a lockable storage area.
- All servers are in lockable locations and managed by DBS-checked staff.
- We lock any back-up tapes in a secure, fire-proof box. Back-ups are encrypted. No back-up tapes leave the site on mobile devices.
- We use RM's solution back-up for disaster recovery on our network / admin, curriculum server(s).
- We comply with the WEEE directive on equipment disposal by using an approved or recommended disposal company for disposal of equipment where any protected or restricted data has been held and get a certificate of secure deletion for any server that once contained personal data.
- Portable equipment loaned by the school (for use by staff at home), where used for any protected data, is disposed of through the same procedure.
- Paper based sensitive information is shredded, using cross cut shredder or collected by secure data disposal service.

6. Equipment and Digital Content

- We have a bank of I-pads which carry the same filtering of the internet as the computers on the school network. No one other than the technician or head teacher is able to download apps.

Personal mobile phones and mobile devices

- Mobile phones should not be in any classroom, toileting area, changing room , or other room used by children. Mobile phones should be placed in staff lockers during their working hours.
- All visitors are requested to keep their phones on silent.
- The recording, taking and sharing of images, video and audio on any mobile phone is to be avoided; except where it has been explicitly agreed otherwise by the headteacher. Such authorised use is to be monitored and recorded.
- The School reserves the right to search the content of any mobile or handheld devices 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 in staff only areas.
- If a staff member is expecting a personal call they may seek specific permissions to use their phone at other than their break times.
- Mobile phones and personally-owned mobile devices brought in to school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personally-owned mobile phones or mobile devices.
- Mobile phones and personally-owned devices are not permitted to be used in pupil used rooms during the school day.
- The Bluetooth or similar function of a mobile phone should be switched off at all times and not be used to send images or files to other mobile phones.
- No images or videos should be taken on mobile phones or personally-owned mobile devices without the prior consent of the Head teacher and person or people concerned.

Students' use of personal devices

- The School strongly advises that student mobile phones should not be brought into school.
- If Students bring mobile phones into school they will be turned off and locked away until the end of the day.
- If a student needs to contact his or her parents or carers, they will be allowed to use a school phone.
- Where it is appropriate to educate students in mobile use, they will be taught to protect their phone numbers by only giving them to trusted friends and family members. Students will be instructed in safe and appropriate use of mobile phones and personally-owned devices and will be made aware of boundaries and consequences.

Staff use of personal devices

- Mobile phones should not be in any classroom, toileting area, changing room , or other room used by children. Mobile phones should be placed in staff lockers during their working hours.
- Staff handheld devices, including mobile phones and personal cameras must be noted in school – name, make & model, serial number.
- Staff are not permitted to use their own mobile phones or devices for contacting children, young people or their families within or outside of the setting in a professional capacity.
- Staff must use a school phone where contact with students, parents or carers is required.
- Mobile Phones and personally-owned devices will be switched off or switched to 'silent' mode. Bluetooth communication should be 'hidden' or switched off and mobile phones or personally-owned devices will be locked in personal lockers during work time. Any use during work time i.e. in emergency circumstances, must have permission of a member of the senior leadership team.
- 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.
- Where staff members are required to use a mobile phone for school duties, for instance in case of emergency during off-site activities, then a school mobile phone will be provided and used. In an emergency where a staff member doesn't have access to a school-owned device, they 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 not identify pupils in online photographic materials or 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 are used on the school web site, 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/filter access to social networking sites or newsgroups unless there is a specific approved educational purpose;
- Staff (and Pupils where appropriate) are advised about how images can be manipulated in their e-Safety education and also told to consider how to publish for a wide range of audiences.

- Staff (and Pupils where appropriate) 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.
- Staff (and Pupils where appropriate) are advised that they should not post images or videos of others without their permission. We explain 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.

Asset disposal

Details of all school-owned hardware will be recorded in a hardware inventory.
Details of all school-owned software will be recorded in a software inventory.
All redundant equipment will be disposed of through an authorised agency. This will include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data.
All redundant equipment that may have held personal data will have the storage media forensically wiped. Alternatively, if the storage media has failed, it will be physically destroyed. The school will only use authorised companies who will supply a written guarantee that this will happen
Disposal of any equipment will conform to The Waste Electrical and Electronic Equipment Regulations 2006 and/or The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007. Further information can be found on the Environment Agency website.

Title	**The Livity School e-safety policy**
Version	**1.0**
Date	**June 2014**
Author	**Carol Argent**
Approved by	**Governing Body**
Next Review Date	**June 2015**

Acceptable Use Policy (AUP):

Adults working with children agreement form

This covers use of digital technologies in The Livity School including email, Internet, intranet and network resources, software, equipment and systems.

- I will only use the The Livity School's digital technology resources and systems for Professional purposes or for uses deemed 'reasonable' by the Senior Leadership team
- I will not reveal my password(s) to anyone.
- I will follow 'good practice' advice in the creation and use of my password. If my password is compromised, I will ensure I change it. I will not use anyone else's password if they reveal it to me and will advise them to change it.
- I will not allow unauthorised individuals to access any of The Livity School's systems.
- I will ensure all documents, data etc., are saved, accessed and deleted in accordance with the The Livity School's network and data security and confidentiality protocols.
- I will not engage in any online activity that may compromise my professional responsibilities.
- I understand that any / my personal online communication tools must not be used with service users and will not communicate or 'befriend' any service user using such methods.
- I will only use the approved email system for any email communication related to work at The Livity School This is currently: LGFL
- I will only use other The Livity School's / Lambeth's approved communication systems for any communication with young people or parents/carers. In this organisation the systems used are: Home school Communication books / phone calls using the school phone system annotated notes taken and given to SLT/ direct face to face communication in school / email communication using approved LGFL email Headteacher cc'd, office staff can also use TEXT anywhere service.
- I will not browse, download or send material that could be considered offensive to colleagues.
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to the appropriate line manager / The Livity School's named contact. This is: Headteacher or SLT
- I will not download any software or resources from the Internet that can compromise the network, or are not adequately licensed.
- I will not publish or distribute work that is protected by copyright.
- I will not connect a computer, laptop or other device (including USB flash drive), to the network / Internet that does not have up-to-date anti-virus software, and I will keep any 'loaned' equipment up-to-date, using the

The Livity School's recommended anti-virus, firewall and other ICT 'defence' systems.

- I will not use personal digital cameras or camera phones for taking and transferring images of young people or staff without permission of the head teacher and will not store images at home without permission.
- I will ensure that any private social networking sites / blogs etc that I create or actively contribute to are not confused with my professional role. I understand that it is my responsibility to ensure I know how to use any such tools so as not to compromise my professional role, such as setting appropriate security settings.
- I will not create a business account on any social networking site unless in full agreement with the appropriate manager, agreed for specific circumstances.
- I agree and accept that any computer or laptop loaned to me by The Livity School, is provided solely to support my professional responsibilities and that I will notify the them of any "significant personal use" as defined by HM Revenue & Customs.
- I will access The Livity School's resources remotely (such as from home) only through approved methods and follow e-security protocols to access and interact with those materials.
- I will ensure any confidential data that I wish to transport from one location to another is protected by encryption and that I follow The Livity School's data security protocols when using any such data at any location.
- I understand that data protection policy requires that any information seen by me with regard to service users, held within the The Livity School's / Lambeth's information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.
- I understand that it is my duty to support a whole organisation safeguarding approach and I will alert the The Livity School's named child protection officer / relevant senior member of staff if I feel the behaviour of any service user or member of staff may be a cause for concern or inappropriate.
- I understand that all Internet usage / and network usage can be logged and this information could be made available to my manager on request.
- I understand that failure to comply with this agreement could lead to disciplinary action.

Acceptable Use Policy (AUP): 'Staff' agreement form

User Signature

I agree to abide by all the points above.

I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the The Livity School's most recent e-safety policies.

I wish to have an email account; be connected to the Intranet & Internet; be able to use the The Livity School's ICT resources and systems.

Signature ..... Date .....

Full Name ..... (printed)

Job title .....

The Livity School .....

Authorised Signature

I approve this user to be set-up.

Signature ..... Date .....

Full Name ..... (printed)

E-safety agreement form: parents

Internet and ICT: As the parent or legal guardian of the pupil(s) named below, I grant permission for the school to give my *daughter / son* access to:

- the Internet at school
- the school's chosen email system (If appropriate)
- ICT facilities and equipment at the school.

I accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the Internet and mobile technologies, but I understand that the school monitors all use of technology and takes every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials.

I understand that the school can, if necessary, check my child's computer files and the Internet sites they visit at school and if there are concerns about my child's e-safety or e-behaviour they will contact me.

Use of digital images, photography and video: I understand the school has a clear policy on "The use of digital images and video" and I support this.

I understand that the school will necessarily use photographs of my child or including them in video material to support learning activities.

I accept that the school may use photographs / video that includes my child in publicity that reasonably promotes the work of the school, and for no other purpose.

I will not take and then share online, photographs of other children (or staff) at school events without permission.

Social networking and media sites: I understand that the school has a clear policy on "The use of social networking and media sites" and I support this.

I understand that the school takes any inappropriate behaviour seriously and will respond to observed or reported inappropriate or unsafe behaviour.

I will support the school by promoting safe use of the Internet and digital technology at home. I will inform the school if I have any concerns.

My daughter / son name(s): _____

Parent / guardian signature: _____

Date: ___/___/___

Guidance for Parents taking Photographs and filming at School Productions

Letters to parents

We are staging a production/special event of on xxxxxx. We are sure some parents/carers would like to take photographs/videos of the production. As you know we have a policy in place with regards to the taking, making and use of images and you will have previously signed a consent form stating whether or not your child could be photographed.

If you wish to take photos at the production there is a strong possibility that other children will also be included within the picture.

At The Livity School we are happy for parents and carers to take photos and video of events for personal use but we request that these images are not distributed or put online. This is to protect all members of the community.

We all enjoy and treasure images of our family and friends; family events, holidays and events are moments we all like to capture in photos or on video. We now have the exciting dimension of adding our images and videos to our online social network, such as Facebook, YouTube and many other websites. This means that we can easily share our photos and video with family and friends.

Whilst this can be very useful to all of us we must ensure we protect and safeguard all children and staff, including those who do not want to have their images stored online.

Please be aware that parents are not permitted to take photographs or to make a video recording for anything other than their own personal use.

- Once posted and shared online any image or video can be copied and will stay online forever.
- Some children are at risk and MUST NOT have their image put online. Not all members of the community will know who they are.
- Some people do not want their images online for personal or religious reasons.
- Some children and staff may have a complex family background which means that sharing their image online can have unforeseen consequences.
- Therefore in order to keep all members of the community safe we must all ‘Think Before We Post’ Online.

The use of digital images and video

To comply with the Data Protection Act 1998, we need your permission before we can photograph or make recordings of your daughter / son.

We follow the following rules for any external use of digital images:

If the pupil is named, we avoid using their photograph.

If their photograph is used, we avoid naming the pupil.

Where showcasing examples of pupils work we only use their first names, rather than their full names.

If showcasing digital video work to an external audience, we take care to ensure that pupils aren't referred to by name on the video, and that pupils' full names aren't given in credits at the end of the film.

Only images of pupils in suitable dress are used.

Staffs are not allowed to take photographs or videos on their personal equipment.

Examples of how digital photography and video may be used at school include:

- Your child being photographed (by the class teacher or teaching assistant) as part of a learning activity;
  e.g. taking photos or a video of progress made by your child, as part of the learning record, and then sharing with their parent / guardian.

- Your child's image being used for presentation purposes around the school;
  e.g. in class or wider school wall displays or PowerPoint© presentations.

- Your child's image being used in a presentation about the school and its work in order to share its good practice and celebrate its achievements, which is shown to other parents, schools or educators;
  e.g. within a CDROM / DVD or a document sharing good practice; in our school prospectus or on our school website.
- In rare events, your child's picture could appear in the media if a newspaper photographer or television film crew attends an event. The Livity School would contact you in advance of this to obtain specific permission.

- If we, or you, actually wanted your child's image linked to their name we would contact you separately for permission.

The use of social networking and on-line media

This school asks its whole community to promote the 3 commons approach to online behaviour:

- **Common courtesy**
- **Common decency**
- **Common sense**

How do we show common courtesy online?

- We ask someone's permission before uploading photographs, videos or any other information about them online.
- We do not write or upload 'off-hand', hurtful, rude or derogatory comments and materials. To do so is disrespectful and may upset, distress, bully or harass.

How do we show common decency online?

- We do not post comments that can be considered as being **intimidating, racist, sexist, homophobic or defamatory. This is cyber-bullying** and may be harassment or libel.
- When such comments exist online, we do not forward such emails, tweets, videos, etc. By creating or forwarding such materials we are all liable under the law.

How do we show common sense online?

- We think before we click.
- We think before we upload comments, photographs and videos.
- We think before we download or forward any materials.
- We think carefully about what information we share with others online, and we check where it is saved and check our privacy settings.
- We make sure we understand changes in use of any web sites we use.
- We block harassing communications and report any abuse.

Any actions online that impact on the school and can potentially lower the school's (or someone in the school) reputation in some way or are deemed as being inappropriate will be responded to.

In the event that any member of staff, student or parent/carer is found to be posting libellous or inflammatory comments on Facebook or other social network sites, they will be reported to the appropriate 'report abuse' section of the network site.
(All social network sites have clear rules about the content which can be posted on the site and they provide robust mechanisms to report contact or activity which breaches this.)

In serious cases we will also consider legal options to deal with any such misuse.

The whole school community is reminded of the CEOP report abuse process: https://www.thinkuknow.co.uk/parents/browser-safety/

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. Listed below are the responses that will be made to any apparent or actual incidents of misuse:

If any apparent or actual misuse appears to involve illegal activity i.e.:

Child sexual abuse images
Adult material, which potentially breaches the Obscene Publications Act
Criminally racist material
Other criminal conduct, activity or materials

The LGfL flow chart – should be consulted and actions followed in line with the flow chart, in particular the sections on reporting the incident to the police and the preservation of evidence.

Pupil Acceptable Use Agreement

Think before you click

S

I will only use the Internet and email with an adult

A

I will only click on icons and links when I know they are safe

F

I will only send friendly and polite messages

E

If I see something I don't like on a screen, I will always tell an adult

My Name:

My Signature: