GOVERNORS OF STAR PRIMARY SCHOOL

ICT & E-Safety Policy

School Mission Statement

At Star Primary School we believe that everyone is equally loved and accepted.

Acknowledging the diversity of our community, we;

- Provide a broad and balance curriculum encouraging every child to take the opportunity to achieve their full potential.
- Nurture positive home, school and community relationships.
- Promote tolerance and respect for all people and the world we live in.

The purpose of this policy is to;

- Set out the key principles expected of all members of the school community at Star Primary School with respect to the use of ICT based technologies.
- Safeguard and protect the children, staff and community of Star Primary 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 online abuse or bullying such as cyber bullying which are cross referenced with other school policies such as our Behaviour Policy.
- 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 pupils.

By order of the Governing Body of Star Primary School

Signed: (Head Teacher) Date: January 2017

Signed: (Chair of Governing Body) Date: January 2017

Policy Date: January 2017 **Review Date: January 2018**

Contents

Introduction and Overview

Our ICT and e-safety policy has been written by the schoo. It also takes into account of advice from CPD attended by the schools SLT, safeguarding and computer learning managers. It has been agreed by the senior management and approved by Governors. It should be reviews annually or sooner dependant on new information and guidance.

ICT in the School Improvement Plan

The key principles of ICT in the School Improvement Plan are to create an exciting and inspiring learning environment with particular focus on Foundation Stage and raise curriculum standards.

Strategic Intent 2016-2017

- To ensure that NQT's receive a very detailed and personalised induction and training.
- To improve the premises and learning environment.
- To redesign and refurbish the existing IT suite.

It is the duty of the school to ensure that every child in their care is safe and that every adult who uses the school site is not vulnerable and that the same principles should apply to the digital world as would be applied to the school's physical buildings. This policy document is drawn up to protect all parties. The pupils and the staff aim to provide clear advice and guidance on how to minimise risks and how to deal with any infringements.

Areas of Risk

The main areas of risk for our school community can be summarised in the following three categories;

Content

- Exposure to inappropriate content, biased online media, online pornography, sexting, exposure to violence, racist language, age ratings and substance abuse.
- Lifestyle websites such as pro-anorexia, self-harm and suicide sites.
- Sites that promote intolerance towards others based on their ethnic background, race, religion, gender etc.
- Erroneous Content: children and adults need to understand how to check authenticity, bias and accuracy of online content.

Content

- Grooming, radicalisation and "stranger danger" through online contacts (social media and websites that promote views that are any of the above).
- All forms of bullying including Cyber Bullying.
- Identity theft, profile hacking and sharing passwords.

Conduct

- Privacy issues such as disclosure of personal information and the promoting of any views that affect community cohesion. [Education and Inspections Act 2006]
- Digital footprint and online reputation.
- Health and well-being such as being aware of how long you spend online.
- Sexting (an act of sending and/or receiving personally intimate messages) also referred to as SGII (self-generated indecent images).
- Copyright infringement and knowing how to take care and consideration for intellectual property and ownership including content, music and film downloads. [Ofsted 2013]

Policy Scope

This policy applies to all members of Star Primary community (staff, students, volunteers, parents/carers, visitors and community users) who have access to and are users of the school ICT system. The Education and Inspections Act (2006) empowers any Head Teacher of a school to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers staff to impose direct disciplinary sanctions for inappropriate behaviour. This is pertinent to incidents of cyber bullying, safeguarding or any other e-safety incidents which may take place outside of the school grounds but still be linked to membership of the school.

The Education Act (2011) increased these powers with regard to searching for and of electronic devices and the deletion of data. The Counter Terrorism and Security Act (2015) placed new statutory duties on schools which means they must work to prevent children being drawn into extremism. The Computer Misuse Act (1990) which covers the use of computer systems without permission or for inappropriate purposes will also be taken account of within this policy.

Under these acts, action can be taken over issues covered by the behaviour and safe guarding policies. The school will deal with such incidents and associated behaviour within its own policies and where appropriate the anti-bullying policy. Where necessary, parents/carers will be informed of incidents that take place outside of the school.

The Head Teacher may decide to report certain matters to the police if a criminal offence is believed to have been committed.

Responsibilities

The Head Teacher will;

- Take overall responsibility for safeguarding provision.
- Take overall responsibility for data and data security as the Senior Information Risk Officer (SIRO).
- Ensure the school uses an approved and filtered internet service which complies with the current requirements.
- Be responsible for ensuring that staff receives suitable training to carry out their e-safety and prevent roles as well as train other colleagues.
- Be aware of procedures to be followed in the event of a serious e-safety and safeguarding incident.
- Receive regular monitoring reports from the child safeguarding officer and computer learning manager.
- Ensure that there is a system in place to monitor and support staff that carry out internal e-safety procedures.

The designated Child Protection Lead will;

- Have day to day responsibilities for safeguarding issues and has a leading role in establishing and reviewing the school safeguarding policies and documents.
- Promote awareness and commitment to e-safeguarding throughout the school community.
- Ensure that e-safety education is embedded across the curriculum.
- Liaise with the school's ICT and technical staff.
- Communicate regularly with SLT and the designated e-safety governor to discuss current issues and review incident logs.
- Ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident.
- Ensure that an e-safety incident log is kept up-to-date.
- Facilitate training and advice for all staff.
- Liaise with the local authority and relevant agencies.
- 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 and/or inappropriate materials
    - Inappropriate on-line contact with adults and/or strangers
    - Potential or actual incidents of grooming
    - Cyber bullying and use of social media

Governors will;

- Ensure that the school follows all current safeguarding and e-safety advice to keep the children and staff safe
- Approve the ICT and E-Safety policy and to review the effectiveness of the policy. This will be carried out by the governors receiving regular updates and information about incidents and monitoring reports.
- Support the school in encouraging parents and the wider community to become engaged in e-safety activities.
- Regularly review e-safety with the school (child protection officer) by looking at incident logs.

Computer Learning Manager will;

- Oversee the delivery of the e-safety element of the computing curriculum.
- Liaise with the child protection officer regularly.
- Report any e-safety related issues that arise to the child protection officer.
- 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.
- Ensure that provision exists for misuse detection and malicious attacks.
- Ensure the security of the school computer system.
- Ensure that access controls and encryption exists to protect personal and sensitive information that is held on school-owned devices.
- Ensure the school's policy on web filtering is applied and updated on a regular basis.
- Inform LGfL of issues relating to filtering applied by the Grid.
- Keep up-to-date with the school's e-safety policy and technical information in order to carry out their e-safety role and to inform and update others.
- Regularly monitor the use of the network, learning environments (MLE), remote access and email accounts to ensure that an misuse/attempted misuse can be reported to the Head Teacher for investigation.
- Ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster.
- Keep up-to-date documentation of the school's e-safety and technical procedures.
- Ensure that all data held on pupils is adequately protected and stored.
- Ensure that all data held on staff and pupils on the school office machines have appropriate access controls in place.
- Ensure compliance with the Data Protection Act.
- Ensure all LGfL services are managed on behalf of the school including maintaining the LGfL USO database of access accounts.

All Staff will;

- Read, understand and help promote the school's e-safety policies and guidance.
- Read, understand, sign and adhere to the school staff acceptable usage policy.
- Be aware of e-safety issues related to the use of mobile phones, cameras and other hand held devices and that they monitor their use and implement current school policies with regard to these devices.
- Report any suspected misuse or problem to the computer learning manager and/or child protection officer.
- Maintain an awareness of current e-safety issues and guidance through CPD.
- Model safe, responsible and professional behaviours in their own use of technology.
- Ensure that any digital communications with pupils should be on a professional level and only through school based systems and never through personal mechanisms.
- Embed e-safety issues in all aspects of the curriculum and other school activities.
- Supervise and guide pupils carefully when engaged in learning activities involved online technology.
- Ensure that all pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws.

All Pupils will;

- Read, understand, sign and adhere to the acceptable usage policy.
- At KS1 it is expected that the parents/carers would sign on behalf of the pupils.
- Have a good understanding of research skills and the need to uphold copyright regulations.
- Understand the importance of reporting abuse, misuse or access to inappropriate materials.
- Know what action to take if they or someone they know feels worried or vulnerable when using online technology.
- Know and understand the school policy on the use of mobile phones, digital cameras and any hand held device.
- Know and understand the school policy on taking and the use of images and on cyber bullying.
- 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.
- Take responsibility for learning about the benefits and risks of using the internet and other technologies safely both in school and at home.
- Help the school in the creation/review of e-safety policies.

Parents/Carers and External Groups will;

- Support the school in promoting e-safety and endorse the acceptable usage policy which includes the pupil's use of the internet and the school's use of photographic and video images.
- Read, understand and promote the school pupil acceptable usage policy with their children.
- Consult with the school if they have any concerns about their children's use of technology.
- Understand the importance of reporting abuse, misuse or access to inappropriate materials to assist the school in supporting e-safety within the community.
- Know what action to take if they or someone they know feels worried or vulnerable when using online technology.
- Any external individual/organisation is expected to sign an acceptable usage policy prior to using any equipment or internet within the school.

Promoting the Policy

The policy will be communicated to staff, pupils and the community in any of the following ways;

1. Policy will be posted on the school website and the MLE.
2. Policy to be included in the induction pack given to new members of staff.
3. Acceptable Usage Agreements discussed with pupils at the start of each year.
4. Acceptable Usage Agreements to be issued to school community usually upon entry to the school.
5. Acceptable Usage Agreement to be held in pupil and personnel files.

Handling Complaints

The school will take all reasonable precautions to ensure e-safety and empower the children to deal with exposure appropriately. However, owing to the international scale and linked nature of internet content, the availability of mobile technologies and the speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or hand held device. Neither the school nor the local authority can accept liability for material accessed or any consequences of internet access.

Staff and pupils are given information about infringements and the possible sanctions in place. Sanctions available include;

- Interview (counselling by the Behaviour Councillor/Phase Group Leader/Child Protection Officer/Deputy Head Teacher/Head Teacher)
- Informing parents/carers.
- Removal of internet and/or computer access for a period of time.
- Referral to the local authority and/or police.

Our child protection officer acts as a first point of contact for any complaint regarding pupil concerns.

Any complaint about staff misuse is referred to the Head Teacher.

Complaints about cyber bullying are dealt with in accordance with out anti-bullying policy.

Complaints related to child protection are dealt with in accordance with the school and local authority child protection procedures.

Review and Monitoring

The e-safety policy is referenced from within other school policies, safeguarding statements, anti-bullying policies and other educational policies. The school has a child protection officer and a computer learning manager who will be responsible for document ownership, review and updates. The e-safety policy will be reviews annually or when any significant changes occur with regards to technology or online threats. The e-safety policy has been written by the computer learning manager and checked by the Head Teacher and the Governors to ensure that it is current and appropriate for its intended audience and purpose. Any changes to the policy will go through a rigorous process of clarification from the Head Teacher and Governors before being edited publicly.

E-Safety in the Curriculum

Star Primary School has a clear and progressive e-safety education programme as part of the computing curriculum. It is built on local authority and LGfL safeguarding and e-literacy framework for EYFS to Year 6 guidance. This covers a range of skills and behaviours appropriate to their age and experience including;

- To understand acceptable behaviour when using an online environment (i.e. be polite, no bad or abusive language or other inappropriate behaviour & keeping personal information private)
- To understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos and to know how to ensure they have turned on privacy settings.
- To STOP and THINK before they CLICK
- To develop a range of strategies to evaluate and verify information before accepting its accuracy.
- To be aware that the author of a web site may have a particular bias or purpose and to develop skills to recognise what that may be.
- To know how to narrow down or refine a search.
- To understand how search engines work and to understand that this affects the results they see at the top of the listings.
- To understand how photographs can be manipulated and how web content can attract the wrong sort of attention.
- 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 must not post pictures or videos of others without their permission.
- To know not to download any files without permission.
- To have strategies for dealing with receipt of inappropriate materials.
- To understand why and how some people will “groom” young people for sexual reasons, exploitation and extremism.
- To understand the impact of cyber bullying, sexting, extremism and trolling and know how to seek help if they are affected by any form of online bullying.
- To know how to report any abuse including cyber bullying and extremism and how to seek help if they experience problems when using the internet and related technologies (i.e. parent/carer, teacher/trusted staff member or an organisation such as CEOP, Child Line or the police).
- Plans internet use carefully to ensure that it is age appropriate and supports the learning objectives for specific curriculum areas.
- Remind pupils about their responsibilities through an acceptable usage policy which every student will sign and will be displayed throughout the school and will regularly be displayed when a student logs on to a school computer.
- Runs projects and events involving pupils to highlight e-safety to parents/carers and pupils.
- 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 and pupils understand issues around bias, copyright and to know they must respect and acknowledge and copyright/intellectual property rights.
- Ensures that staff and pupils understand the issues around aspects of the commercial use of the internet, as age appropriate. This may include risks in pop-ups, buying online, online gaming and online gambling.
- Provides information and advice sign posted on the school website.

Staff and Governor Training

Star Primary School will;

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

Parent Awareness Training

Star Primary School runs a programme of advice and guidance for parents including;

- An introduction of the Acceptable Use Agreements to new parents, to ensure that principles of e-safe behaviour are made clear
- Information leaflets; articles in the school newsletters and on the school web site.
- Suggestions for safe Internet use at home.
- Providing information about national support sites for parents.
- Information and advice sign posted on the school website.

Safeguarding and Prevent Strategy

Star Primary School;

- Ensures that through our school vision, values, rules, diverse curriculum and teaching we promote tolerance and respect for all cultures, faiths and lifestyles.
- Ensures that staff understands the issues of radicalisation, are able to recognise the signs of vulnerability or radicalisation and know how to refer their concerns.
- Ensures that staff and pupils understand the issues around aspects grooming, exploitation and radicalisation on the Internet, as age appropriate.
- Is aware that extremists use the internet, including social media, to share their messages and takes appropriate steps to reduce exposure.
- Refer to and keep up to date with our prevent duties as set out below.

Statutory Duties

- The duty to prevent children and young people being radicalised is set out in the following documents.
- Counter Terrorism and Security Act (2015)
- Keeping Children Safe in Education (2015)
- Prevent Duty Guidance (2015)
- Working Together to Safeguard Children (2015)

Non-Statutory Guidance

- Promoting fundamental British values as part of SMSC in schools: Departmental advice for maintained schools (DfE 2014)

Conduct and Incident Management

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. (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 be 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

In this school, staff/students/pupils;

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

In this school, 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

At Star Primary 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.
- Sanctions are applied according to the policy that applies to that contravention unless a serious incident that involves a criminal act occurs at which point the matter will be directed to the police without regard for internal management procedures.
- 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 (e.g. LGfL, 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 LA / 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.
- Any incident that indicates that evidence of indecent images or offences concerning child protection involving members of the school community should be immediately referred to the

Police. This is to prevent the loss of valuable evidence both on and off the premises by not inadvertently making the suspect aware of raised suspicions.

Managing the ICT Infrastructure

Internet Access, Security & Filtering

Star Primary 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 are logged and only available to staff with the approved 'web filtering management' status.
- Uses USO user-level filtering where relevant, thereby closing down or opening up options appropriate to the age / stage of the pupils.
- Ensures network healthy 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, and 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 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.
- Uses security time-outs on Internet access where practicable / useful.
- 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 (MLE) and 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; e.g. yahoo for kids or ask for kids, Google Safe Search.
- Never allows/is vigilant when conducting 'raw' image search with pupils e.g. Google image search.
- Informs all users that Internet use is monitored; o Informs staff and students that that they must report any failure of the filtering systems directly to the CLMs. Our Nominated Contacts 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

Star Primary School;

- Uses individual, 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.
- Ensures the Computer Learning Managers are up-to-date with LGfL services and policies. We also require Newham Partnership Working (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.

New and Emerging Technology

Star Primary School;

- Will access new and emerging technologies for educational benefit and a risk assessment taking into account our safeguarding criteria will be carried out before use in school is allowed.

Ensuring the network is used safely

Star Primary 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 username and password for access to our school's network.
- Control Staff access to the schools' management information system through a separate password for data security purposes.
- Provide pupils with an individual network log-in username. From Year 3 they are also expected to use a personal password.
- Give all pupils their own unique username and password which gives them access to the Internet and the Learning Platform.
- We use the London Grid for Learning's Unified Sign-On (USO) system for username and passwords.
- Make it clear that no one should log on as another user and make it 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; 15 ICT and E-Safety Policy2015.
- Have 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.
- Require all users to always log off when they have finished working or are leaving the computer unattended.
- Request 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.
- Have set-up the network so that users cannot download executable files / programmes.
- Have blocked access to music/media download or shopping sites – except those approved for educational purposes.
- Scan all mobile equipment with anti-virus / spyware before it is connected to the network.
- Make clear that members of staff is 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.
- Make it clear that staff ensure 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 CLMs; equipment installed and checked by approved Suppliers / LA electrical engineers.
- Have separate curriculum and administration networks, with access to the Management Information System set-up so as to ensure staff users can only access modules related to their role; e.g. teachers access Attendance.
- 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, 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 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.
- 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); 16 ICT and E-Safety Policy2015
- Follow LGfL 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 were phased out of the school by late 2016 and replaced with interactive touchscreens which have a much longer life.

Personal Password/Email Accounts

Password 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 it.
- 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 SIMS system.
- We require staff to change their passwords into the MIS and LGfL USO admin site.

Email

Star Primary School;

- Provides staff with an email account for their professional use, London Staff mail and 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, for example info@star.newham.sch.uk (with one or more staff having access to an aliased/shared mailbox for 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.
- Will report 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 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

- We use LGfL London Mail with pupils and lock this down where appropriate using LGfL Safe Mail rules.
- Pupils' LGfL London Mail e-mail accounts are intentionally 'anonymised' for their protection.
- Pupils are introduced to, and use e-mail as part of the ICT/Computing scheme of work.
- Year R/1 pupils are introduced to principles of e-mail through the Visual Mail facility in the London LEARNING PLATFORM OR closed 'simulation' software.
- Pupils can only receive external mail from, and send external mail to, addresses if the Safe Mail 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.
- 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.
- 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.

- All staff are required to 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 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 authorised website managers [Computer Learning Managers and Office Manager] but only once approved by the Head teacher.
- 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, e.g. info@star.newham.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 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.
- E-Safety Advice and help is sign posted from the school site to support the whole school community.

MLE and LGfL Learning Platform

- Uploading of information on the schools' MLE is shared between different staff members according to their responsibilities e.g. all class teachers upload information in their class areas.
- Photographs and videos uploaded to the schools MLE will only be accessible by members of the school community.
- In school, pupils are only able to upload and publish within school approved and closed systems, such as the MLE.

CCTV

- We have CCTV in the school as part of our site surveillance for staff and student safety. We will not reveal any recordings (retained for 28 days), without permission except where disclosed to the Police as part of a criminal investigation.
- We may occasionally review footage to check on health and safety matters as part of our normal safeguarding or practice review. This is used to improve the outcome for all users.
- All images are stored and processed in compliance with the Data Protection Act and are only kept for a limited period.

Social Media and 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, but to use the schools' preferred system for such communications.
- The school will control access to social media and social networking sites.
- Pupils will be advised never to give out personal details of any kind which may identify them and/or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and email addresses, full names of friends/family, specific interests and clubs etc.
- Staff wishing to use Social Media tools with students as part of the curriculum will need permission from the Head teacher or SLT before using Social Media tools in the classroom. They will need to risk assess the sites before use and check the sites terms and conditions to ensure the site is age appropriate.
- Staff official blogs or wikis should be password protected and run from the school website with approval from the Senior Leadership Team.
- Personal publishing will be taught via age appropriate sites [such as J2Bloggy] that are suitable for educational purposes. They will be moderated by the school where possible.
- Pupils will be advised on security and privacy online and will be encouraged to set passwords, deny access to unknown individuals and to block unwanted communications. Pupil will be encouraged to approve and invite known friends 19 ICT and E-Safety Policy2015 only on social networking sites and to deny access to others by making profiles private.
- All members of the school community are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.
- Concerns regarding students' use of social networking, social media and personal publishing sites (in or out of school) will be raised with their parents/carers, particularly when concerning students' underage use of sites.

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

Star Primary School;

- Will when required to do so only use the LGfL supported services for video conferencing activity.
- Only uses approved or checked webcam sites

Data Security

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

Strategic and Operational Practices

At Star Primary School;

- The Head Teacher is the Data Controller and Senior Information Risk Officer (SIRO).
- Staff are clear who are the key contact(s) for key school information / Data Managers are.
- We ensure staff know who to report any incidents where data protection may have been compromised.
- All staff are Disclosure and Barring Service (DBS) and Disqualification by Association (DbA) checked and records are held in one central record e.g. SIMS. We ensure ALL the following school stakeholders sign an Acceptable Use Agreement form. We have a system so we know who has signed. 20 ICT and E-Safety Policy2015
    - Staff
    - Governors
    - Pupils
    - Parents
    - This makes clear staff 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.
- School staff with access to setting-up usernames and passwords for email, network access and Learning Platform access are working within the approved system and follow the security processes required by those systems.
- We ask staff to undertake at least annual house-keeping to review, remove and destroy any digital materials and documents which need no longer be stored.

Technical Solutions

All staff have access to 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 minutes idle time on the network.
- We use the DfE S2S site to securely transfer CTF pupil data files to other schools.
- Staff with access to the Admissions system also uses a LGfL OTP tag as an extra precaution.
- We use RAv3 with its 2-factor authentication for remote access into our systems.
- We use LGfL 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.
- No back-ups leave the site on mobile devices.
- We use NPW remote secure back-up solution for disaster recovery on our network servers.
- 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.
- 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.

Equipment and Digital Content

All school mobile devices that connect through the school's wireless access points are subjected to the same filtration and monitoring system as those devices that gain access to the internet through conventional authenticate network connections.

Personal mobile phones and mobile devices

- Student mobile phones which are brought into school must be turned off (not placed on silent) and handed to the Reception staff on arrival at school. These can be collected at the end of the day.
- Staff members may use their phones during school break times.
- Designated 'mobile use free' areas are situated in the school, and signs to this effect are to be displayed throughout. The areas which should be considered most vulnerable include: toilets, bathrooms and in some settings - sleep areas and changing areas.
- Mobile phones brought into school are entirely at the staff member, pupil' & 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.
- 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 Head teacher. Such authorised use is to be monitored and recorded. All mobile phone use is to be open to scrutiny and the Head Teacher 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 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 pupils 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. If a staff member is expecting a personal call they may leave their phone with the school office to answer on their behalf, or seek specific permissions to use their phone at other than their 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.
- 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 certain areas within the school site, e.g. changing rooms and toilets.
- 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 from the Head Teacher.

Pupils' use of personal devices

- The School strongly advises that pupil mobile phones and other portable devices should not be brought into school.
- The School accepts that there may be particular circumstances in which a parent wishes their child to have a mobile phone for their own safety.
- If a pupil breaches the school policy then the phone or device will be held in a secure place in the school office. Mobile phones and devices will be released to parents or carers in accordance with the school policy.
- Phones and devices must not be taken into examinations. Pupils found in possession of a mobile phone during an exam will be reported to the appropriate examining body. This may result in the pupil's withdrawal from either that examination or all examinations.
- If a pupil needs to contact his or her parents or carers, they will be allowed to use a school phone. Parents are advised not to contact their child directly during the school day, but to contact the school office.
- Pupils should protect their phone numbers by only giving them to trusted friends and family members. Pupils will be instructed in safe and appropriate use of mobile phones and personally-owned devices and will be made aware of boundaries and consequences.
- Personal devices that can store; share and/or transmit data or content should not be brought into school without prior consent from staff. It may be confiscate, searched and any inappropriate content deleted or shared with the authorities by the head teacher or appointed representative.

Staff use of personal devices

- Staff handheld devices, including mobile phones and personal cameras must be noted in school – name, make & model, serial number. Any permitted images or files taken in school should be downloaded from the device and deleted in school before the end of the day.
- Staff discouraged from using their own mobile phones or devices for contacting pupils or their families in their professional capacity.
- Staff members are encouraged to use a school phone where contact with pupils, parents or carer is required. If it can't be avoided staff should use the 141 prefix to avoid disclosing their private number.
- Mobile Phones and personally-owned devices should be switched off or switched to 'silent' mode.
- Bluetooth communication should be 'hidden' or switched off.
- If members of staff have an educational reason to allow children to use mobile phones or a personally-owned device as part of an educational activity then it will only take place when approved by SLT.
- Staff should avoid using personally-owned devices, such as mobile phones or cameras, to take photos or videos of pupils and should 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, or for contacting pupils or parents, then a school phone will be provided and used.
- Where a staff member does not 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

At Star Primary 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 (not group 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.
- 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 pupils as part of their ICT scheme of work.
- Pupils and Staff 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 identity 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, grooming or abuse.

Asset Disposal

- Details of all school-owned hardware are recorded in a hardware 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.

Additional Information

London Grid for Learning (LGfL) offer advice and guidance on best practice for member schools and we liaise with them closely on a day to day basis.
[www.lgfl.net/safety]

Child net International, a non-profit organisation, offer advice for children, parents and professionals. [http://www.childnet.com/]

Alternatively refer to your Union for advice, support and guidance.

Title	Star Primary School – ICT & E-Safety Policy
Date	27 January 2017
Author	M Norton (Computer Learning Manager)
Approved by;	
	L von Buchenroder (Head Teacher)
	S Hendricks (Chair of Governors)
Next Review Date	January 2018