ST. THERESA'S CATHOLIC PRIMARY SCHOOL

Online Safety Policy

Our Mission Statement

At St. Theresa's School
We learn together
We play together
We pray together
We grow together in the love of God.

Date of policy review: July 2019
Next review: July 2020

Policy written by: James Troy
Policy reviewed & passed by: Governing Body
Key person responsible Linda O'Melia Headteacher

Contents

1. Introduction and overview 3
   - 1.1. Rationale and Scope 3
   - 1.2. Roles and Responsibilities 4
   - 1.3. How the policy will be communicated to staff/pupils/community 6
   - 1.4. Handling Complaints 6
   - 1.5. Review and Monitoring 7

2. Education and Curriculum 7
   - 2.1. Pupil e-safety Curriculum 7
   - 2.2. Staff and Governor Training 8
   - 2.3. Parent/Carer Awareness and Training 8

3. Expected Conduct and Incident Management 8
   - 3.1. Expected Conduct 9
   - 3.2. Incident Management 9

4. Managing the ICT infrastructure 10
   - 4.1. Internet Access, Security (virus protection) and Filtering 10
   - 4.2. Network Management (user access, backup) 11
   - 4.3. Passwords Policy 12
   - 4.4. E-mail 12
   - 4.5. School Website 14
   - 4.6. Learning Platform 15
   - 4.7. Social Networking 15
   - 4.8. Video Conferencing 15
   - 4.9. CCTV 15

5. Data Security 15
   - 5.1. Management Information System access 15
   - 5.2. Data transfer 16

6. Equipment and Digital Content 17
   - 6.1. Personal Mobile Phones and Devices 17
     - 6.1.1. Pupils Use of Personal Devices 17
     - 6.1.2. Staff Use of Personal Devices 18
   - 6.2. Digital Images and Video 18
   - 6.3. Asset Disposal 19

Appendices:

I. Acceptable Use Agreement (Staff)
II. Acceptable Use Agreement (Pupils)
III. Acceptable Use Agreement including photo/video permission (Parents/Carers)
IV. Protocol for responding to e-safety incidents

1. Introduction and Overview

1.1 Rationale and Scope

This policy aims to:

- Set out the key principles expected of all members of the school community at St Theresa's RC Primary school with respect to the use of information computer technology (ICT) based technologies.
- Safeguard and protect the children and staff of St Theresa's RC 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 such as cyberbullying which are cross referenced with other school policies.
- 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.

The main areas of risk for our school community can be summarised as follows (from Ofsted, 2013):

Content

- Exposure to inappropriate content, including online pornography, substance abuse, violence and ignoring age ratings in games, (exposure to violence associated with often racist language).
- Lifestyle websites, for example pro-anorexia/self-harm/suicide sites/radicalisation.
- Hate sites.
- Content validation: how to check authenticity and accuracy of online content.

Contact

- Grooming.
- Cyber-bullying in all forms.
- Identity theft including: 'frape' (hacking Facebook profiles); 'brape', (hacking Blackberry Messenger (BBM)); and sharing passwords.

Conduct

- Privacy issues, including disclosure of personal information.
- Digital footprint and online reputation.
- Health and well-being, (amount of time spent online (internet or gaming)).
- Sexting, (sending and receiving of personally intimate images), also referred to as SGII (self generated indecent images).
- Copyright, (little care or consideration for intellectual property and ownership – such as music and film).

Scope

- This policy applies to the whole school community including St Theresa's RC Primary school's Senior Leadership Team, school board of governors, all staff employed directly or indirectly by the school and all pupils.

- The Education Act 2011 gives the school the power to confiscate and search the contents of any mobile device if the Headteacher believes it contains any material that could be used to bully or harass others.
- The school will clearly detail its management of incidents within this policy, associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate safeguarding behaviour that takes place out of school.

1.2 Roles and responsibilities

Role	Key Responsibilities
Headteacher	• To take overall responsibility for e-Safety provision. • To take overall responsibility for Data Security (Senior Information Risk Owner (SIRO)). • To ensure the school uses an approved, filtered Internet Service, which complies with current statutory requirements. • 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).
e-Safety Co-ordinator / Child Protection Officer	• 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 Senior Leadership Team (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 (LA), 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 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/carers and the wider community to become engaged in e-safety activities.

Role	Key Responsibilities
	• 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). • To take responsibility for 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. – London Grid for Learning (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 (VLE) FRONTER/LGFL email is regularly monitored in order that any misuse/attempted misuse can be reported to the E-Safety Co-ordinator and Headteacher for investigation and action. • 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.
Managed Learning Environment Leader (MLE)	• To ensure that all data held on pupils on the MLE is adequately protected.
Data Manager	• To ensure that all data held on pupils on the school office machines have appropriate access controls in place.
Universal Sign-On (USO) Nominated contact(s)	• To maintain the USO database of access accounts.
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, extracurricular 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. • 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.

Role	Key Responsibilities
	• 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. • To ensure that any digital communications with pupils should be on a professional level and only through school-based systems, never through personal mechanisms, e.g. email, text, mobile phones etc.
Pupils	• Read, understand, sign and adhere to the Pupil Acceptable Use Policy (nb. at KS1 it would be expected that parents/carers would sign on behalf of the pupils). • Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations. • To 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. • To take responsibility for learning about the benefits and risks of using the internet and other technologies safely both in school and at home. • To help the school in the creation/ review of e-safety policies.
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's Pupil Acceptable Use Agreement with their children. • To access the school website/VLE/on-line pupil records 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.

1.3 How the policy be communicated to staff/pupils/community

- The St Theresa's RC Primary school's senior leadership team will be responsible for ensuring all members of school staff and pupils are aware of the existence and contents of the school eSafeguarding policy and the use of any new technology within school.
- The eSafeguarding policy will be provided to and discussed with all members of staff formally.
- The eSafeguarding policy will be introduced to the pupils at the start of each school year through assemblies and/or class lessons.
- The eSafeguarding policy will be made available to parents/carers via the school website or MLE.

1.4 Handling Complaints

- Staff and pupils are given information about infringements in use and possible sanctions. Sanctions available include:
  - Interview with e-Safety Coordinator and Headteacher.
  - Informing parents/carers.
  - Removal of Internet or computer access for a period.
  - Referral to Local Authority Designated Officer (LADO)/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.

1.5 Review and Monitoring

- The school eSafeguarding policy has been agreed by the SLT and approved by governors.
- The eSafeguarding policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the school.

2. Education and Curriculum

At St Theresa's RC Primary school:

- We foster a 'No Blame' environment that encourages pupils to tell a teacher or responsible adult immediately if they encounter any material that makes them feel uncomfortable.
- We teach pupils and inform staff what to do if they find inappropriate web material i.e. to switch off monitor and report the Uniform Resource Locator (URL), to the teacher.

2.1 Pupil e-Safety curriculum

- We have a clear, progressive e-safety education programme as part of the Computing curriculum, throughout all Key Stages, built on the LGfL e-Safeguarding and e-literacy framework for EYFS to Y6. This covers a range of skills and behaviours appropriate to their age and experience, including:
  - 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/page 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.
  - For older pupils to understand how search engines work and to understand that this affects the results they see at the top of the listings.
  - 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 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 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 understand why they must not post pictures or videos of others without their permission.
  - To know not to download any files – such as music files - without permission.
  - To have strategies for dealing with receipt of inappropriate materials.
  - For older pupils to understand why and how some people will 'groom' young people for sexual reasons.
  - To understand the impact of cyberbullying, sexting 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 cyberbullying; and how to seek help if they experience problems when using the internet and related technologies, i.e. parent/carer, teacher or trusted staff member, or an organisation such as Childline or the CLICK CEOP (Child Exploitation and Online Protection) button.
- Any internet use will be carefully planned to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.
- Pupils will be taught how to use a range of age-appropriate online tools in a safe and effective way.
- We will remind pupils about their responsibilities through an end-user Acceptable Use Policy which every pupil will sign/will be displayed throughout the school/will be displayed when a pupil logs on to the school network.
- Staff will model safe and responsible behaviour in their own use of technology during lessons.

2.2 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.
- To use where necessary for emailing sensitive data.
- Makes regular training available to staff on e-safety issues and the school's e-safety education programme.
- 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.

2.3 Parent/Carer Awareness and Training

This school

- Runs a rolling programme of advice, guidance and training for parents/carer, including:
  - Introduction of the Acceptable Use Agreements to new parents/carers, 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/carers.
  - Regular newsletter with current E-Safeguarding information.

3. Expected Conduct and Incident Management

- All staff sign our 'Staff Acceptable Use Agreement' to say they have read and understood the e-safety policy and guidance on handling e-safety incidents.
- All children in KS1 and KS2 have been read and understand the acceptable use agreements.
- Parents/carers sign the 'Parents e-Safety Agreement' giving permission for pupils to use ICT, mobile devices and online resources and for the school to use digital images for school purposes.
- The school will maintain an e-Safety incident log.
- Staff must report any failure of the web filtering systems directly to the e-Safety Co-ordinator (Headteacher) who will escalate as appropriate to the Barnet Schools ICT Support or LGfL (Atomwide).
- Headteacher must refer any material we suspect to be illegal to the appropriate authorities ie. Police and the LADO.
- Staff supervise pupils' use of the internet at all times.

- Staff always preview websites before use.
- Staff plan the curriculum context for Internet use selecting appropriate websites and avoid open web-searching.
- We ensure that when copying materials from the web, staff and pupils understand issues around plagiarism; how to check copyright and also know that they must observe and respect copyright / intellectual property rights.
- In accordance with our anti-bullying policy pupils are encouraged to tell a member of staff if there is a cyber-bullying incident.
- Staff should keep copies of any abusive material as evidence, tell the child not to respond and then follow the school anti-bullying policy for reporting.
- If it is a serious case involving threat or intimidation the Headteacher may need to report it to the police.
- If staff become aware that a child may have put themselves in vulnerable position through their online behaviour (eg underage use of Facebook, uploading videos to Youtube, contacting strangers online) it must be reported to the e-Safety Co-ordinator (Headteacher).
- If a staff member becomes aware of any inappropriate behaviour or use of digital technology by an adult in school, they must report it to the e-Safety Co-ordinator .

3.1 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, (at KS1 it would be expected that parents/carers would sign on behalf of the pupils).
- Need to understand the importance of misuse or access to inappropriate materials and are aware of the consequences.
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's 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.

Pupils

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

Parents/Carers

– should provide consent for pupils to use the Internet, as well as other technologies, as part of the 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.

3.2 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 LA 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/Local Safeguarding Children Board (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

4.1 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.
- 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 LGfL approved system USO FX 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 pupils.
- 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 pupils 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 FRONTER/the London MLE/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 pupils to age/subject appropriate web sites; Plans the curriculum context for Internet use to match pupils' ability, using child-friendly search engines where more open Internet searching is required; eg yahoo for kids or ask for kids , Google Safe Search.
- Is vigilant when conducting 'raw' image search with pupils e.g. Google image search.
- Informs all users that Internet use is monitored.
- Informs staff and pupils that that they must report any failure of the filtering systems directly to E-Safety Officer. Our system administrator(s) logs or escalates as appropriate to the Technical service provider or LGfL (Atomwide) 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/carers.
- Immediately refers any material we suspect is illegal to the appropriate authorities – Police – and the LA.

4.2 Network Management (user access, backup)

This school,

- Uses individual, audited log-ins for all users - the London USO system.
- Uses teacher 'remote' management control tools for controlling workstations/viewing users / setting-up applications and Internet web sites, where useful.
- Has additional local network auditing software installed.
- Ensures the Systems Administrator/network manager is up-to-date with LGfL services and policies/requires the Technical Support Provider to be up-to-date with LGfL services and policies.

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.
- Staff access to the schools' management information system is controlled through a separate password for data security purposes.
- We provide pupils with an individual network log-in username. From Year 1 they are also expected to use a personal password.
- All pupils have their own unique username and password which gives them access to the Internet and FRONTER, the Learning Platform.
- We use the LGfL USO system for username and passwords.
- Makes clear that no one should log on as another user and makes clear that pupils should never be allowed to log-on or use teacher and staff logins as these have far less security restrictions and inappropriate use could damage files or the network.
- Has set-up the network with a shared work area for pupils and one for staff. Staff and pupils are shown how to save work and access work from these areas.
- Requires all users to always log off when they have finished working or are leaving the computer unattended.
- Where a user finds a logged-on machine, we require them to always log-off and then log-on again as themselves.

- Requests that teachers and pupils switch off computers after use to ensure complete log off.
- Has set-up the network so that users cannot download executable files/programmes.
- Has blocked access to music download or shopping sites – 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. e.g. teachers access report writing module; SEN coordinator - SEN data.
- 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/carers 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.
- Has a clear disaster recovery system in place for critical data that includes a secure, remote back up of critical data, that complies with external Audit's requirements.
- Uses the Department for Education (DfE), secure s2s website for all common transfer files (CTF), 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 LA 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.

4.3 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.

4.4 E-mail

This school

- Provides staff with an email account for their professional use : LGfL 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@schoolname.la.sch.uk / head@schoolname.la.sch.uk / or class e-mail addresses, (with one or more staff having access to an aliased/shared 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.
- Manages accounts effectively with up to date account details of users.
- 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 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 LondonMail with pupils and lock this down where appropriate using LGfL SafeMail rules.
- Pupils' LGfL LondonMail 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.
- 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.
- 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.

4.5 School Website

- The Headteacher takes overall editorial 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 ICT technicians, specialist TA.
- The school web site complies with the school's 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@schooladress or admin@schooladress. 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 expect teachers using' school approved blogs or wikis to password protect them and run from the school website.

4.6 Learning Platform

- Uploading of information on the schools' Learning Platform / virtual learning space 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 Learning Platform.

4.7 Social Networking

- Teachers are instructed not to run social network spaces for pupil use on a personal basis or to open up their own spaces to their pupils, but to use the schools' Learning Platform for such communications.

School staff will ensure that:

- No reference should be made in social media to 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 or LA.
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

4.8 Video Conferencing

This school

- Only uses the LGfL/NEN service for video conferencing activity.
- Only uses approved or checked webcam sites.

4.9 Closed Circuit Television (CCTV)

- We have CCTV in the school as part of our site surveillance for staff and pupil 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.

5. Data security

5.1 Management Information System Access

At this school:

- The Headteacher is the Senior Information Risk Officer (SIRO).
- Staff are clear who are the key contact(s) for key school information (the Information Asset Owners) are. We have listed the information and information asset owners in a spreadsheet.
- 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 *name of MIS* e.g. Integris G2, Personnel or spreadsheet.
  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,
  - pupils,

– parents/carers

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

5.2 Data Transfer

- We follow LA guidelines for the transfer of any data, such as MIS data or reports of children, to professionals working in the LA 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.
- 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 undertaken at least annual house-keeping to review, remove and destroy any digital materials and documents which need no longer be stored.
- 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 the Pan-London Admissions system (based on USO FX), to transfer admissions data.
- Staff with access to the Admissions system also use a LGfL OTP tag as an extra precaution.
- 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, Atomwide's AutoUpdate, for creation of online user accounts for access to broadband services and the London MLE,.
- We store any Protect and Restricted written material in lockable storage cabinets 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 cabinet. Back-ups are encrypted. No back-up tapes leave the site on mobile devices.
- We use LGfL's GridStore remote secure back-up/named alternative solution> 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 system hard drives 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.
- We are using secure file deletion software.

6. Equipment and Digital Content

6.1 Personal mobile phones and devices

- Designated 'mobile use free' areas are situated in the setting, 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's and parents/carers 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.
- Pupil mobile phones which are brought into school must be turned off, (not placed on silent), and stored in the office upon arrival. They must remain turned off and out of sight until the end of the day. Staff members may use their phones during school break times. 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. All mobile phone use is to be open to scrutiny and the Headteacher 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/carers 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.
- Mobile phones will not be used during lessons or formal school time unless as part of an approved and directed curriculum-based activity with consent from a member of staff.
- The Bluetooth 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.
- Personal mobile phones will only be used during lessons with permission from the teacher.
- No images or videos should be taken on mobile phones or personally-owned mobile devices without the prior consent of the person or people concerned.
- All mobile phones and personally-owned devices will be handed in at reception should they be brought into school.

6.1.1 Pupils' use of personal devices

- The School strongly advises that pupil mobile phones should not be brought into school.
- The School accepts that there may be particular circumstances in which a parent/carer 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 confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to parents/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/carers, they will be allowed to use a school phone. Parents/carers are advised not to contact their child via their mobile phone 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.
- Pupils will be provided with school mobile phones to use in specific learning activities under the supervision of a member of staff. Such mobile phones will be set up so that only those features required for the activity will be enabled.
- No pupils should bring his or her mobile phone or personally-owned device into school. Any device brought into school will be confiscated.

6.1.2 Staff use of personal devices

- 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 will be issued with a school phone where contact with pupils, parents/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 not be used during teaching periods unless permission has been granted by a member of the senior leadership team in emergency circumstances.
- 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 the senior leadership team.
- 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/carers, 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.

6.2 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.
- Digital images/video of pupils are stored in a private teachers' shared images folder on the network and images are deleted at the end of the year – unless an item is specifically kept for a key school publication.
- 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.
- 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 eSafety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents/carers or younger children as part of their ICT scheme of work.
- Pupils are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.
- Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identify of others and their location, such as house number, street name or school. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.

6.3 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 ICT 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 ICT equipment that may have held personal data will have the storage media overwritten multiple times to ensure the data is irretrievably destroyed. 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 ICT 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.