St Catherine's RC Primary School: Internet Safety Policy January 2017

St Catherine's Catholic Primary School

Vale Drive, Barnet, Hertfordshire, EN5 2ED

Telephone 020 8440 4946

Fax 020 8441 4346

Title	St Catherine's Internet safety policy
Version	1.1
Date	08/01/2017
Author	Josh David internet safety coordinator
Approved by head teacher	Maureen Kelly
Approved by Governing Body	
Next Review Date	January 2018

Modification History			
Version	Date	Description	Revision Author
0.1	22/10/2015	Review	Josh David e-safety coordinator
0.2	08/01/2017	review	Josh David internet safety leader

Contents

1. Introduction and Overview

Rationale
This policy aims to:

- set out the key principles expected of all members of the school community at St Catherine's RC Primary school with respect to the use of ICT-based technologies.
- safeguard and protect the children and staff of St Catherine'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 cyber-bullying 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 students.

The main areas of risk for our school community can be summarised as follows:

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
- hate sites and sites of an extremist nature
- content validation: how to check authenticity and accuracy of online content
- Children using apps which have an age restriction above their own age.

Contact

- grooming
- cyber-bullying in all forms
- identity theft 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 Catherine's RC Primary school's Senior Leadership Team, school board of governors, all staff employed directly or indirectly by the school and all students.

- The Education Act 2011 gives the school the power to confiscate and search the contents of any mobile device if the head teacher 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 and carers of incidents of inappropriate internet Safety behaviour that takes place out of school.

Roles and responsibilities

Role	Key Responsibilities
Head teacher	• To take overall responsibility for internet Safety provision • To take overall responsibility for Data Security (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 internet safety roles and to train other colleagues, as relevant • To be aware of procedures to be followed in the event of a serious internet Safety incident. • To receive regular monitoring feedback from the internet Safety leader • To ensure that there is a system in place to monitor and support staff who carry out internal internet safety procedures. • To ensure any new pupils or staff to the school have agreed to and signed any relevant policies
Internet Safety leader	• takes day to day responsibility for internet safety issues and has a leading role in establishing and reviewing the school internet safety policies / documents • promotes an awareness and commitment to internet safety throughout the school community • ensures that internet safety education is embedded across the curriculum • liaises with school ICT technical staff • To communicate regularly with SLT and the designated internet Safety Governor / committee to discuss current issues • To ensure that all staff are aware of the procedures that need to be followed in the event of an internet Safety incident • To ensure that an internet Safety incident is referred to the head teacher and then logged according to the school logging procedures. • facilitates training and advice for all staff • liaises with the Local Authority and relevant agencies • Is regularly updated in internet safety issues and legislation, and be aware of the potential for serious child protection issues to arise

	Governors / Internet safety governor	• To ensure that the school follows all current internet Safety advice to keep the children and staff safe • To approve the internet Safety Policy and review the effectiveness of the policy. This will be carried out by the Governors / Governors Sub Committee receiving regular information about internet safety incidents and monitoring reports. A member of the Governing Body has taken on the role of internet Safety Governor • To support the school in encouraging parents and the wider community to become engaged in internet safety activities
	Computing Curriculum Leader	• To oversee the delivery of the internet safety element of the Computing curriculum
	Network Manager/tech Nician/support technician	• To report any internet Safety related issues that arise, to the internet Safety leader. • 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 · LGfL is informed of issues relating to the filtering applied by the Grid · that he / she keeps up to date with the school's internet safety policy and technical information in order to effectively carry out their internet 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 internet Safety leader and Head teacher 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 internet security and technical Procedures • To record any items purchased or destroyed in the relevant inventory and make sure that the inventory is up to date.

Role	Key Responsibilities
Data leader/coordinator	• To ensure that all data held on pupils on school technologies have appropriate access controls in place. • To ensure that all data held on pupils on the MLE is adequately protected
ICT support technician	• To maintain the USO database of access accounts • To maintain safe search filters on the school network • To ensure that staff have secure passwords in place for all sensitive sites. • To dispose of images and other media storage of children on the school website at the end of every academic year.
Teachers	• To deliver all of the internet safety objectives for their year group in the course of the academic year • To embed internet safety issues in all aspects of the curriculum and other school activities • To supervise and guide pupils carefully when engaged in learning activities involving online technology (including, extra curricular and extended school activities if relevant) • To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws • To report any internet safety concerns to the internet safety leader and head teacher immediately.
All staff	• To read, understand and help promote the school's internet Safety policies and guidance • To read, understand, sign and adhere to the school staff Acceptable Use Agreement • To be aware of internet safety issues related to the use of mobile phones and other internet capable devices and that they monitor their use and implement current school policies with regard to these devices • To report any suspected misuse or problem to the internet Safety leader and head teacher • To maintain an awareness of current internet 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 Student / Pupil Acceptable Use Policy and the mobile phone 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 internet safety practice when using digital technologies out of school and realise that the school's internet 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

Role	Key Responsibilities
Parents/carers	• to support the school in promoting internet safety To 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 endorse the mobile phone policy: this includes children's and adults' use. • to read, understand and promote the school Pupil Acceptable Use Agreement with their children • to access the school website and use parent pay in accordance with the relevant school Acceptable Use Agreement. • to consult with the school if they have any concerns about their children's/other children's/staff members 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. Any external individual / organisation will verbally agree to the mobile phone policy before being allowed to enter the school building.
Office staff	• To make sure anyone who enters the school premises is either verbally read or has the opportunity to read the school mobile phone safety policy before entering the school premises. • To ensure the school mobile phone policy section, which details adult use of mobile phones is visibly displayed outside the school office.

How the policy be communicated to staff/pupils/community

- The St Catherine's RC Primary school's senior leadership team will be responsible for ensuring all members of school staff and students are aware of the existence and contents of the school internet Safety policy and the use of any new technology within school.
- The internet Safety policy will be provided to and discussed with all members of staff formally.
- The pupil acceptable use agreement and mobile phone use agreement will be introduced to the students at the start of each by either the head teacher or members of the SLT in assemblies.
- The internet Safety policy will be made available to parents or carers via the school Website.

Handling complaints

- Staff and pupils are given information about infringements in use and possible sanctions. Sanctions available include:
  - Interview with internet Safety leader and Head teacher;
  - informing parents or carers;
  - removal of Internet or computer access for a period
  - referral to LADO / Police.

- Our internet Safety leader acts as first point of contact for any complaint. Any complaint about staff misuse is referred to the Head teacher.

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

Review

- The school internet Safety policy has been agreed by the senior leadership team and approved by governors.
- The internet Safety 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

Ethos
At St Catherine's RC Primary school 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 URL to the teacher .

Pupil internet Safety curriculum

- We have a clear, progressive internet safety education programme as part of the Computing curriculum, throughout all Key Stages, built on the LGfL 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 cyber-bullying, 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 cyber-bullying; and how to to seek help if they experience problems when using the internet and related technologies, i.e. parent or carer, teacher or trusted staff member, or an organisation such as Child line or the CLICK CEOP button.
- Any internet use will be carefully planned to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.

- Students will be taught how to use a range of age-appropriate online tools in a safe and effective way.
- We will remind students about their responsibilities through an end-user Acceptable Use Policy which every student will sign/will be displayed throughout the school/will be displayed when a student logs on to the school network.
- Staff will model safe and responsible behaviour in their own use of technology during lessons.
- Students will be taught how to report any concerns they have about the internet.

Staff and governor training
This school

- Ensures staff know how to send or receive sensitive and personal data and understand the requirement to encrypt data where the sensitivity requires data protection
- Makes regular training available to staff on internet safety issues and the school's internet safety education program.
- Provides, as part of the induction process, all new staff [including those on university/college placement and work experience] with information and guidance on the internet Safety policy and the school's Acceptable Use Policies.
- To ensure that when sensitive information is emailed, the proper and secure email system is used.

Parent awareness and training

This school

- Runs a rolling programme of advice, guidance and training for parents, including:
    - Introduction of the Acceptable Use Agreements to new parents, to ensure that principles of internet 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.
    - Regular newsletter with current internet safety information

3. Expected Conduct and Incident management

- All staff sign our 'Staff Acceptable Use Agreement' to say they have read and understood the internet safety policy and guidance on handling internet safety incidents
- All children in Foundation, KS1 and KS2 have been read and understand the acceptable use agreements.
- Parents sign the 'Parents acceptable use Agreement' giving permission for pupils to use Technologies and online resources and for the school to use digital images for school purposes;
- The school will log internet safety issues in line with school policy on logging behaviour/safeguarding incidents

- Staff must report any failure of the web filtering systems directly to the internet Safety leader and Headteacher who will escalate as appropriate to the Barnet Schools ICT Support or LGfL (Atomwide)
- The 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 Head teacher may need to report it to the police;
- If staff become aware that a child may have put themselves in a vulnerable position through their online behaviour (eg underage use of Facebook, uploading videos to Youtube, contacting strangers online) it must be reported to the internet Safety leader and 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 internet Safety leader and headteacher .

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 internet safety practice when using digital technologies out of school and realise that the school's internet 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 internet capable devices and cyber bullying.

Staff

- are responsible for reading the school's internet safety policy and using the school ICT systems accordingly.

Students/Pupils

- should have a good understanding of research skills, what is and isn't acceptable internet use, what cyber-bullying is and how to respond to cyber bullying, how to stay safe online, how to report concerns 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 internet safety acceptable use agreement form at time of their child's entry to the school
- should know and understand what the 'rules of appropriate use' are and what sanctions result from misuse

Incident Management
In this school:

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

4. Managing the ICT infrastructure

- Internet access, security (virus protection) and filtering

This school:

- Has the educational filtered secure broadband connectivity through the LGfL and so connects to the 'private' National Education Network;
- Uses the LGfL Net Sweeper filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature,

etc. All changes to the filtering policy is logged and only available to staff with the approved 'web filtering management' status;

- Uses USO user-level filtering where relevant, thereby closing down or opening up options appropriate to the age / stage of the students;.
- 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 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
- Requires staff to preview websites before use [where not previously viewed or cached] and encourages use of the school's Learning Platform as a key way to direct students to age / subject appropriate web sites; Plans the curriculum context for Internet use to match pupils' ability, using child-friendly search engines where more open Internet searching is required; eg Google Safe Search
- Is vigilant when conducting 'raw' image search with pupils e.g. Google image
- Informs all users that Internet use is monitored;
- Informs staff and students that that they must report any failure of the filtering systems directly to 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
- Immediately refers any material we suspect is illegal to the appropriate authorities – Police – and the LA.

- Network management (user access, backup)
  This school
  - Uses individual, audited log-ins for all 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 internet 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 the Learning Platform.
- We use the London Grid for Learning's Unified Sign-On (USO) system for username and passwords;
- Makes clear that no one should log on as another user and makes clear that pupils should never be allowed to log-on or use teacher and staff logins as these have far less security restrictions and inappropriate use could damage files or the network;
- Has set-up the network with a shared work area for pupils and one for staff. Staff and pupils are shown how to save work and access work from these areas;
- Requires all users to always log off when they have finished working or are leaving the computer unattended;
- Where a user finds a logged-on machine, we require them to always log-off and then log-on again as themselves.
- 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 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 DfE secure s2s website for all CTF files sent to other schools;
- Ensures that all pupil level data or personal data sent over the Internet is encrypted or only sent within the approved secure system in our LA or through USO secure file exchange (USO FX);
- Follows 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.

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.

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 /
- 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:

- Pupils are introduced to, and use e-mail as part of the ICT/Computing scheme of work.
- Pupils can only receive mail from, and send mail to, email addresses of other pupils at St Catherine's

- Pupils are taught about the safety and 'netiquette' of using e-mail both in school and at home.
* 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 personal emails to transfer staff or pupil personal data. We use secure, LA / DfE approved systems.
- All staff sign our LA / school Agreement Form AUP to say they have read and Understood the internet safety rules

- u

School website

- The Headteacher takes overall editorial responsibility to ensure that the website content is accurate and the quality of presentation is maintained;
- 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
- 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

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

At this school:

- The Head Teacher 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

  This makes clear staffs' responsibilities with regard to data security, passwords and access.
- We follow LA guidelines for the transfer of any data, such as MIS data or reports of children, to professionals working in the Local Authority or their partners in Children's Services / Family Services, Health, Welfare and Social Services.
- We require that any Protect and Restricted material must be encrypted if the material is to be removed from the school and limit such data removal. / We have an approved remote access solution so staff can access sensitive and other data from home, without need to take data home.
- 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 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 harddrives 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>.

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 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;
- 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.

Asset disposal

- Details of all school-owned hardware will be recorded in a hardware inventory by the ICT technician
- Details of all school-owned software will be recorded in a software inventory by the ICT technician.
- 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.

Tracking

DfE Stat Policy	Best Practice	Web	MyUSO	Signed by Staff	Version
-	✓	✓	✓	✓	1.0
-	✓	✓	✓	✓	1.1