Trafalgar Schools' Federation

Trafalgar Infant School **Trafalgar Junior School**

	Name of school	Trafalgar Schools' Federation
	Online safety policy review date	Summer 2018
	Date of next review	Summer 2019
	Who reviewed this policy	Jane Burton

Trafalgar Infant School Online Safety Policy

Contents

1. Introduction and Overview

Rationale

The purpose of this policy is to:

- Set out the key principles expected of all members of the school community at **Trafalgar Schools' Federation** with respect to the use of ICT-based technologies.
- Safeguard and protect the children and staff of **Trafalgar Schools' Federation.**
- 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 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 students.

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

Content

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

Contact

- Grooming (including sexual exploitation, radicalisation etc.)
- Online bullying in all forms
- Social or commercial identity theft, including password

Conduct

- Aggressive behaviours (bullying)
- 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

This policy applies to all members of the Trafalgar Schools' Federation community (including staff, students/pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of Trafalgar Schools' Federation IT systems, both in and out of Trafalgar Schools' Federation

Roles and responsibilities

Role	Key Responsibilities
Headteacher: L. Thompson	• Must be adequately trained in ofline and online safeguarding, in-line with statutory guidance and relevant Local Safeguarding Children Board (LSCB) guidance • To lead a 'safeguarding' culture, ensuring that online safety is fully integrated with whole school safeguarding. • To take overall responsibility for online safety provision • To take overall responsibility for data management and information security (SIRO) ensuring school's provision follows best practice in information handling • To ensure the school uses appropriate IT systems and services including, filtered Internet Service, e.g. LGfL services and those provided by Gaia • To be responsible for ensuring that all staff receive suitable training to carry out their safeguarding and online safety roles • To be aware of procedures to be followed in the event of a serious online safety incident • Ensure suitable 'risk assessments' undertaken so the curriculum meets needs of pupils, including risk of children being radicalised • To receive regular monitoring reports from the Online Safety Lead • To ensure that there is a system in place to monitor and support staff who carry out internal online safety procedures, e.g. network manager and online safety lead • To ensure Governors are regularly updated on the nature and effectiveness of the school's arrangements for online safety • To ensure school website includes relevant information.

Role	Key Responsibilities

Online safety leads:
J. Burton and J. Allen
	• Takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies / documents
	• Promotes an awareness and commitment to online safety throughout the school community
	• Ensures that online safety education is embedded across the curriculum
	• Liaises with school ICT technical staff where appropriate
	• To communicate regularly with the Headteacher and the designated online safety Governor 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 online safety incident
	• To ensure that an online safety incident log is kept up to date
	• Facilitates training and advice for all staff on online safety issues.
	• Oversees any pupil surveys/pupil feedback/parent surveys regarding online safety questions
	• Liaises with the Local Authority and relevant agencies
	• Is regularly updated on online safety issues and legislation, and is 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

Online safety governor: S. Bradley	• To ensure that the school has in place policies and practices to keep the children and staff safe online • To approve the Online Safety Policy and review the effectiveness of the policy. This will be carried out by the PPC and Resources Governors Sub Committee receiving regular information about online safety incidents and monitoring reports. • To support the school in encouraging parents and the wider community to become engaged in online safety activities through workshops, website andlearning platform where relevant. • The role of the online safety Governor will include an annual review with the online safety lead and will include the online safety incident log.
ICT/Computing Leads: J. Burton and S. Sloan & V. Jain	• To oversee the delivery of the online safety element of the Computing curriculum • To liaise with staff to keep this up to date and relevant and ensure staff feel confident in delivering it. • To ensure that all data held on pupils on our learning platform (where there is one) is adequately protected • To liaise with DPO to ensure we are GDPR compliant.

Role	Key Responsibilities
Network technician: Gaia	• To report any online safety related issues that arises, to the online safety lead • To report online safety related issues that come to their attention, to the Online Safety Leads • To manage the school's computer systems, ensuring - school password policy is strictly adhered to. - systems are in place for misuse detection and malicious attack (e.g. keeping virus protection up to date) - 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 (currently provided by LGFL) • That they keep up to date with the school's online safety policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant • That the use of school technology is regularly monitored and that any misuse/attempted misuse is reported to the online safety Leads at Trafalgar Infant and Junior School or the Headteacher • To ensure appropriate backup procedures and disaster recovery plans are in place • To keep up-to-date documentation of The Federation's online security and technical procedures.
Data Manager:s D.Staynes and N. Ghosh DPO: B.Taylor	• To ensure that the data they manage is accurate and up-to-date • Ensure best practice in information management. i.e. have appropriate access controls in place, that data is used, transferred and deleted in-line with data protection requirements. • Both schools must be registered with Information Commissioner.
LGFL Nominated contacts J.Burton and L.Thompson J. Allen and S.Sloan	• To ensure all LGfL services are managed on behalf of the school
All staff	• To embed online safety throughout the curriculum • 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 pupils are aware of the importance of respectful use of online content, including copyright and plagiarism.

Role	Key Responsibilities
All staff, students, and regular volunteers and contractors who have unsupervised contact with the children.	• To read, understand, sign and adhere to the school's online safety, Top Tips Sheet and Acceptable Use Agreement and discuss this is relation to our full online safety policy on induction. • To be aware of online 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 regards to these devices • To report any suspected misuse or problem to the online safety leads (J. Burton and J. Allen) • To maintain an awareness of current online safety issues and guidance e.g. through CPD • To model safe, responsible and professional behaviours in their own use of technology • Will not change the setup of school devices (e.g. passwords and pins) without discussing this with the online safety/ICT leads • 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. non-school. email, text, mobile phones etc. **Exit strategy** , At the end of the period of employment to return any equipment or devices belonging to the school, including (where relevant) leaving PIN numbers, IDs and passwords to allow devices to be reset.
Pupils	• Read, understand, sign and follow the Pupil Staying Safe Online agreement • To be aware of the importance of respectful use of online content, including copyright and plagiarism and the difference between opinion, fact and fiction • To know what action to take if they or someone they know feels worried or vulnerable when using online technology and talk to someone they know they can trust. • To know and understand school policy on the use of mobile phones, digital cameras and hand-held devices. • To know and understand school policy on the taking / use of images and on cyber-bullying. • To understand the importance of adopting safe behaviours and good online safety practice when using digital technologies out of school and realise that the school's online safety policy covers their actions out of school • To contribute to any 'pupil voice' / surveys that gathers information of their online experiences.

Role	Key Responsibilities
Parents/carers	• To support the school in promoting online safety and endorse the Parents' Acceptable Use Agreement which includes the pupils' use of the Internet and the school's use of photographic and video images • To read, understand and promote the school Pupil Staying Safe Online agreement (SSO)with their children • To consult with the school if they have any concerns about their children's use of technology • To access any school websites or learning platforms 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 Agreement prior to using any equipment or the Internet within school • to support the school in promoting online safety • To model safe, responsible and positive behaviours in their own use of technology.

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

- Policy to be posted on the school website/ learning platform
- A summary of the policy is part of our red safeguarding folder (top tips)
- Policy to be part of school induction pack for new staff
- Acceptable Use Agreements and Staying Safe Online agreements discussed with staff and pupils at the start of each year and copies of the signing sheet are in kept in staff Green Folder
- Acceptable Use Agreements to be issued to whole school community, usually on entry to the school and filed with profiles.
- A copy of the SSO (Staying Safe Online agreement) will also be kept in:

Infant School - the children's reading diaries/journals and Computing books.
Junior School - the children's Home School Links Book.

Handling complaints:

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

- Staff and pupils are given information about infringements in use and possible sanctions. Sanctions available include:
    - Interview by online safety Leads
    - informing parents or carers;
    - removal of Internet or computer access for a period,
    - referral to LA / Police.

- Our Online safety Leads act as first point of contact for any complaint. Any complaint about staff misuse is referred to the Headteacher.

- 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 by either the school's online safety lead or the school's safeguarding /deputy safeguarding leads

Review and Monitoring

- The online safety policy is referenced from within other school policies including the ICT and Computing policy, Child Protection policy, Behaviour policy, including the Anti-Bullying, Personal, Social, Health and Economic Education and Citizenship policy and School Development Plans
- Policy review and updates will be managed by the Federation's online safety leads
- The online safety policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within across the Federation
- The online safety policy has been written by the Federation online safety Leads and is current and appropriate for its intended audience and purpose.
- There is widespread ownership of the policy and it has been agreed by the Headteacher and approved by Governors and other stakeholders. All amendments to the school online safety policy will be discussed in detail with all members of teaching staff.

Version Control

As part of the maintenance involved with ensuring our online safety policy is updated revisions will be made to the document annually as part of our review cycle. Please see the table on the front of this policy for version control information.

2. Education and Curriculum

Pupil online safety curriculum

Trafalgar Schools' Federation

- Has a clear, progressive online safety education programme as part of the Computing curriculum/PSHE&C and other curriculum areas as relevant. 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 (fact, opinion, fiction)
    - 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 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 that if it is unacceptable offline it is unacceptable online
    - 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;
    - To understand the impact of cyber bullying 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 seek help if they experience problems when using the Internet and related technologies, i.e. parent or carer, teacher or trusted staff.

- Plans Internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.
- Will remind students about their responsibilities through an end-user Staying Safe Online agreement (SSO) which every student will sign and will be displayed throughout the school, in their reading diaries/journals, Computing books and Home School Links Book depending on whether they are EYFS/KS1 or KS2
- Ensures staff will model safe and responsible behaviour in their own use of technology during lessons.

- Ensures that when copying materials from the web, staff and pupils understand issues around plagiarism; how to check copyright and know that they must respect and acknowledge copyright / intellectual property rights;
- Ensures that staff and pupils understand the issues around aspects of the commercial use of the Internet, as age appropriate. This may include, risks in pop-ups; buying on-line; on-line gaming / gambling;

Staff and governor training

This school

- Ensures staff know how to send or receive sensitive and personal data and understand the requirement to encrypt data where the sensitivity requires data protection and use password protected storage devices where necessary.
- Makes regular training available to staff on online safety issues and the school's online safety education programs: staff meetings/INSET sessions/regular updates and start of year revision of procedures
- 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 online safety policy and the school's Acceptable Use Agreement.

Parent awareness and training

This school

- Runs a rolling programme of advice, guidance and training for parents, including:
    - Introduction of the Acceptable Use Agreement and Staying Safe Online agreement to new parents, to ensure that principles of online safe behaviour are made clear
    - Information leaflets; in school newsletters on the school website and on the school learning platform (where relevant)
    - demonstrations, practical sessions held at school;
    - suggestions for safe Internet use at home;
    - provision of information about national support sites for parents.
    - Online safety updates throughout the year are either uploaded to the online safety page in the Parent information room on the e-school or directly on the School website and parents are signposted to these via the weekly school newsletter

3. Expected Conduct and Incident management

Expected conduct

At Trafalgar Schools' Federation

all users:

- Are responsible for using the school IT and communication systems in accordance with the relevant Acceptable Use Agreement which they will be expected to sign before being given access to school systems 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 online safe practice when using digital technologies out of school and realise that the school's online safety Policy covers their actions out of school, if related to their membership of the school
- Will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand-held devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying

Staff

- Are responsible for reading the school's online safety policy and Top Tops sheet and using the school IT and communication systems accordingly, including the use of mobile phones, and hand-held devices.
- Know to be vigilant in the supervision of children at all times, as far as is reasonable, and uses common-sense strategies in learning resource areas as set out in the school's Top Tips sheet
- Know to take professional, reasonable precautions when working with pupils, previewing websites before use; using age-appropriate (pupil friendly) search engines where more open Internet searching is required with younger pupils;

Parents/Carers

- Should provide consent for pupils to use the Internet, as well as other technologies, as part of the online safety Acceptable Use Agreement / Staying Safe Online agreement (SSO) 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

Within this Federation:

- There is strict monitoring and application of the online 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 (e.g. the local authority, the LA online safety adviser LGFL, UK Safer Internet Centre helpline, CEOP, NSPCC and other relevant agencies.
- Monitoring and reporting of online safety incidents takes place and contribute to developments in policy and practice in online safety within the school. The records are reviewed/audited and reported to the school's senior leaders, Governors /the LA / LSCB where appropriate.
- Parents / carers are specifically informed of online 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
- We will immediately refer any suspected illegal material to the appropriate authorities – Police, Internet Watch Foundation and inform the LA.

4. Managing the IT and Communication System

Internet access, security (virus protection) and filtering

The Federation:

- Has the educational filtered secure broadband connectivity through the LGfL
- Uses the LGfL filtering system which blocks sites that fall into categories (e.g. adult content, race hate, gaming). All changes to the filtering policy are logged and only available to staff with the approved 'web filtering management' status;
- Uses USO user-level filtering where relevant, thereby closing down or opening up options appropriate to the age / stage of the students;
- ensures network health through use of Sophos anti-virus software (from LGfL) etc. and network set-up so staff and pupils cannot download executable files;
- Uses DfE, LA or LGfL approved systems including DfE S2S, LGfL USO FX2, Egress secure file/email to send 'protect-level' (sensitive personal) data over the Internet
- Uses encrypted devices or secure remote access where staff need to access 'protect-level' (sensitive personal) data off-site;
- Bocks 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.
- Has blocked pupil access to music download or shopping sites – except those approved for educational purposes at a regional or national level, such as Audio Network;

- Works in partnership with the LGfL to ensure any concerns about the system are communicated so that systems remain robust and protect students;
- Is vigilant in its supervision of pupils' use at all times, as far as is reasonable, and uses common-sense strategies in learning resource areas where older pupils have more flexible access;
- Ensures all staff and students have signed an Acceptable Use Agreement and Staying Safe Online agreement (SSO) and understands that they must report any concerns;
- Ensures pupils only publish within an appropriately secure environment: the school's learning environment and LGfL secure platforms such as J2Bloggy and similar sites agreed by the school
- Requires staff to preview websites before use [where not previously viewed or cached]and if not to turn off the interactive board/panel when searching Encourages use of the school's Learning Platform as a key way to direct students to age / subject appropriate web sites; Plans the curriculum context for Internet use to match pupils' ability, using child-friendly search engines where more open Internet searching is required; e.g. yahoo for kids or ask for kids , Google Safe Search , …..
- 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 students that that they must report any failure of the filtering systems directly to the online safety lead who will log or escalate as appropriate.
- 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 Federation

- Uses individual, audited log-ins for all users created by LGFL/Atomwide and used for network, e-school and software login at EYFS and KS1 and additional logins at KS2
- Uses guest accounts for external or short-term visitors for temporary access to appropriate services such as school networks and learning platforms.
- Ensures the Systems Administrator/network manager is up-to-date with LGfL services and policies/requires the Technical Support Provider to be up-to-date with LGfL services and policies

- Storage of all data within the school will conform to the UK data protection requirements
- Pupils and Staff using mobile technology, where storage of data is online, will conform to the EU data protection directive where storage is hosted within the EU.

To ensure the network is used safely, Trafalgar Schools' Federation

- Ensures staff read and sign that they have understood the relevant parts of the Federation's online safety Policy. Following this, they are set-up with Internet, email access and network access. Online access to service is through a unique, audited username and password. We also provide a different username and password for access to our school's network
- Ensures staff access to the schools' management information system is controlled through a separate password for data security purposes;
- Provides pupils with an individual network log-in username and password. These are introduced at an appropriate time based on discussion between staff and online safety lead.
- Ensures all pupils have their own unique username and password which gives them access to the school network.
- Uses the London Grid for Learning's Unified Sign-On (USO) system for username and passwords at EYFS & KS1 and has begun to migrate this over to KS2
- 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 personal 'my docs' for each student to save their work in.
- 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. All staff logins are timed out after a period of inactivity requests that teachers and pupils do not switch the computers off during the day unless they are unlikely to be used again that day or have completely crashed. We also automatically switch off all computers at 9 o'clock to save energy and allow for updates
- Has set-up the network so that users cannot download executable files / programmes;
- Has blocked access to music/media 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 equipment installed and checked by approved Suppliers / LA electrical engineers
- Has integrated curriculum and administration networks, but access to the Management Information System is set-up so as to ensure staff users can only access modules related to their role;
- Ensures that access to the school's network resources from remote locations by staff is restricted and access is only through school / LA approved systems (e.g.) RAv3 and Office 365
- 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 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 our broadband network for our CCTV system and have had set-up by approved partners;
- Uses the DfE secure s2s website for all CTF files sent to other schools;
- Ensures that all pupil level data or personal data sent over the Internet is encrypted or only sent within the approved secure system in our LA or through USO secure file exchange (USO FX);
- Follows ISP advice on Local Area and Wide Area security matters and firewalls and routers have been configured to prevent unauthorised use of our network;
- Our wireless network will be 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 (where applicable) are maintained so that the quality of presentation remains high;
- Reviews the school IT and communication systems regularly with regard to health and safety and security.

Password policy

This Federation

- Makes it clear that staff and pupils must always keep their password private, must not share it with others and must not leave it where others can find it.
- Ensures all staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password private.
- Requires relevant staff to change their passwords into the MIS, LGfL USO admin site secure every 90 days.

E-mail

This Federation

- Provides staff with an email account for their professional use and makes clear personal email should be through a separate account;
- Has the ability to provide highly restricted Safe mail for pupil's email use e-mail
- Does not publish personal e-mail addresses of pupils or staff use anonymous or group e-mail addresses, for example ict@trafalgar-inf.richmond.shc.uk for communication with the wider public.
- Will contact the Police if one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law.
- Will ensure that email accounts are maintained and up to date
- Reports messages relating to or in support of illegal activities to the relevant Authority and if necessary to the Police.
- Will use the report spam tab embedded within our school email accounts where necessary
- 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.

When Safemail is used Pupils:

- are taught about the safety and 'netiquette' of using e-mail both in school and at home i.e. they will be taught to use LGfL Safe Mail and we will use LGfL SafeMail rules to provide a safe email environment
- if Safe mail is used pupils can only receive external mail from, and send external mail to, addresses if the SafeMail rules have been set to allow this.
- email safety and netiquette includes:
    - 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;
    - 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 Staying Safe Online agreement (SSO) to say they have read and understood the online safety rules, including e-mail, and we explain how any inappropriate use will be dealt with.

Staff:

- Staff can only use the LGfL e mail system on the school system
- Staff only use LGfL e-mail system for professional purposes
- Access in school to external personal e mail accounts may be blocked
- 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. 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 school Acceptable Usage Agreement AUA to say they have read and understood the online safety rules, including e-mail and we explain how any inappropriate use will be dealt with.

School website

- The Headteacher supported by the Governing Board takes overall responsibility to ensure that the website content is accurate, and the quality of presentation is maintained;
- Uploading of information is restricted to our website authorisers and overseen by the HeadTeacher
- The school web site complies with the statutory DfE guidelines for publications.
- Most material is the school's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status;
- The point of contact on the web site is the school address, telephone number and we use a general email contact address, e.g. info@schooladdress or admin@schooladdress. Home information or individual e-mail identities will not be published;
- Photographs published on the web do not have full names attached;
- We do not use pupils' names when saving images in the file names or in the tags when publishing to the school website;
- We do not use embedded geodata in respect of stored images
- We expect teachers to use school approved blogs such as J2bloggy Learning platform/Cloud Environments
- Uploading of information on the schools' Learning Platform 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 learning platform will only be accessible by members of the school community;
- In school, pupils are only able to upload and publish within school approved systems such as the blogs and Learning Platforms;

Social networking

- Staff are advised to always keep professional and private communication separate
- Staff are advised not to run social network spaces for student use on a personal basis or to open up their own spaces to their students, but to use the schools' learning platform for such communications.
- for the use of any school approved social networking will adhere to school's communications policy.

School staff will ensure that in private use:

- 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 local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.
- They do not engage in online discussion on personal matters relating to members of the school community;
- In order for any concerns or complaints to be resolved as quickly and fairly as possible, staff will not discuss them publicly via social media. Concerns and complaints will be dealt with confidentially for those involved, and we expect complainants to observe confidentiality also.

Parents

- Parents are reminded about social networking risks and protocols through our parental Acceptable Use Agreement and additional communications materials when required.
- Are reminded that they are not to upload photographs, videos or any other information about other people.

Pupils

- Are taught about social networking, acceptable behaviours and how to report misuse, intimidation or abuse through our online safety curriculum work.
- Students are required to sign and follow our [age appropriate] pupil Staying Safe Online agreement (SSO)

Video Conferencing
Trafalgar Infant School:

- Will check with the online safety Lead and/or the Headteacher before taking part in video conferencing to ensure safety is not compromised.
- Only uses approved or checked webcam sites;

- We use specialist lesson recording equipment on occasions as a tool to share best teaching practice. We do not reveal any such recordings outside of the staff and will not use for any other purposes.

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

Strategic and operational practices

At this school:

- The Head Teacher is the Senior Information Risk Officer (SIRO).
- 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 a single central register

  We ensure ALL the following school stakeholders sign an AUA / SSO. We have a system so we know who has signed.

  - staff,
  - governors,
  - pupils
  - parents
  - Volunteers (if they are working with children unsupervised)
  - students
  - work experience students
  - external clubs

  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 Protected 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 undertake regular reviews to remove and destroy any digital materials and documents which need no longer be stored.

Technical Solutions

- Staff have a secure area 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 60 minutes idle.
- We use password protected 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 an LGfL OTP tag (or soft OTP option) as an extra precaution.
- We currently use LGFL RAv3 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, USO Auto Update, for creation of online user accounts for access to broadband services and the London content
- We store 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 for disaster recovery on our network
- We comply with the WEEE directive on equipment disposal by using an approved or recommended disposal company for disposal of equipment where any protected or restricted data has been held
- Portable equipment loaned by the school (for use by staff at home), where used for any protected data, is disposed of through the same procedure.
- Paper based sensitive information is shredded, using a cross cur shredder and collected by secure data disposal service.
- We are using secure file deletion software.

6. Equipment and Digital Content

Personal mobile phones and mobile devices
Staff use

- 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 brought into school are entirely at the staff member, parents' or visitors own risk. The School accepts no responsibility for the loss, theft or damage of any phone or hand-held device brought into school.
- All visitors are requested to keep their phones turned off.
- Visitors are not permitted to use their mobile phones (or other devices) to photograph or video any members of the school community without prior permission being sort from the Headteacher.
- The recording, taking and sharing of images, video and audio on any mobile phone by a member of staff is to be avoided. If a personal device is used by a member of staff then all images must be deleted by the end of the day and may not be shared via Wi-Fi, Bluetooth or other such wireless technology with anyone outside of school
- 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 or students need to contact each other during the school day, they should do so only through the School's office. 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 permission from the Headteacher to use their phone at other than their break times.
- Personal devices should not be used to access or respond to phone calls, emails, texts or social media sites whilst responsible for children and should be switched off or on silent. Staff may use their device to share media with the children to support/enhance pupil learning but must do so via an IWB/panel/computer/or television not directly on their device.

- 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 students or parents, they should hide (by inputting 141) their own mobile number for confidentiality purposes.
- If a member of staff breaches the school policy, then disciplinary action may be taken.

Students' use of personal devices

- The Federation does not currently permit students to bring their own devices in to use in school. Should this change then pupils would be required to follow the guidelines set out below as advised by LGFL
- Year 5 and 6 pupils are permitted to bring a phone to school but it must be switched off and handed in to the class teacher on arrival.

Asset disposal

Details of all school-owned hardware will be recorded in a hardware inventory.
Details of all school-owned software will be recorded in a software inventory.
All redundant equipment will be disposed of through an authorised agency. This will include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data.
All redundant equipment that may have held personal data will have the storage media forensically wiped. Alternatively, if the storage media has failed, it will be physically destroyed. The school will only use authorised companies who will supply a written guarantee that this will happen