Policy for
E-Safety

Contents

1. Introduction and Overview
   - Rationale and Scope
   - Roles and responsibilities
   - How the policy will be communicated to staff/pupils/community
   - Handling complaints
   - Review and Monitoring

2. Education and Curriculum
   - Pupil Online Safety curriculum
   - Staff and governor training
   - Parents awareness and training

3. Expected Conduct and Incident Management

4. Managing the IT Infrastructure
   - Internet access, security (virus protection) and filtering
   - Network management (user access, backup, curriculum and admin)
   - Passwords policy
   - E-mail
   - School website
   - Social networking
   - Video Conferencing

5. Equipment and Digital Content
   - Personal mobile phones and devices
   - Digital images and video
   - Asset disposal

Appendices:

Governor Responsibility:	Learning & Community Committee
Staff Responsibility:	A Ashraf
Review Period:	Bi-annual
Status:	Non-statutory
Reviewed:	Spring 2016
Next Review Date:	Autumn 2018
Governor Signature	

1. Introduction and Overview

Rationale
The internet and other digital technologies permeate all aspects of life in a modern technological society. Internet use is part of the statutory National Curriculum and is a necessary tool for staff and pupils. It is the entitlement of every pupil to have access to the internet and digital technologies, in order to enrich his/her learning.

- set out the key principles expected of all members of the school community at Tetherdown with respect to the use of IT-based technologies.
- safeguard and protect the children and staff of Tetherdown
- 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 online 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, 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
- online bullying in all forms
- identity theft (including 'frape' (hacking Facebook profiles)) 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)
- extremism
- copyright (little care or consideration for intellectual property and ownership – such as music and film)

Scope

This policy applies to all members of Tetherdown community (including staff, students / pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school systems, both in and out of Tetherdown.

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

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

Role	Key Responsibilities
Headteacher	Responsible for e-safety issues within the school but may delegate the day-to-day responsibility to other members of Teaching Staff. •Ensure that the Governing Body is informed of e-safety issues and policies. •Ensure that appropriate funding is allocated to support e-safety activities throughout the school.

E Safety Co-ordinator / Designated Child Protection Lead	• 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 safeguarding throughout the school community.
	• ensures that Online safety education is embedded across the curriculum.
	• liaises with school Computing technical staff.
	• To communicate regularly with SLT and the designated Governor committee to discuss current issues, review incident 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.
	• liaises with the Local Authority and relevant agencies
	• To oversee the delivery of the online safety element of the Computing curriculum.
	• 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
	  • Online bullying and use of social media
	Educating Parents and raising awareness as instructed by Head.

Learning and Community	E-Safety will be reviewed as part of the regular review of child protection and health and safety policies.

Role	Key Responsibilities
Committee (Governors)	•Support the headteacher and/or designated e-safety co-ordinator in establishing and implementing policies, systems and procedures for ensuring a safe ICT learning environment. •Ensure that appropriate funding is authorised for e-safety solutions, training and other activities as recommended by the headteacher and/or designated e-safety coordinator (as part of the wider remit of the Governing Body with regards to school budgets).
Network Manager/technician	• To report any online safety related issues that arise, to the Online 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 ensure the security of the school IT 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 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 the *network / PLATFORM) / remote access / email* is regularly monitored in order that any misuse / attempted misuse can be reported to the *Online Safety Co-ordinator / Officer /Headteacher for investigation / action / sanction* • To ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster. • To keep up-to-date documentation of the school's online security and technical procedures
Business Manager	• To ensure that all data held on pupils on the school office machines have appropriate access controls in place
LGfL Nominated contact(s)	• To ensure all LGfL services are managed on behalf of the school including maintaining the LGfL USO database of access accounts.
Teachers	• To embed online safety issues in all aspects of the curriculum and other school activities • To supervise and guide pupils carefully when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant) • To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws
All staff	• To read, understand and help promote the school's e-safety policies and guidance • To read, understand, sign and adhere to the school staff Acceptable Use Agreement • 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 regard to these devices • To report any suspected misuse or problem to the online safety coordinator • 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

Role	Key Responsibilities
	• 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 (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 reporting abuse, misuse or access to inappropriate materials • to know what action to take if they or someone they know feels worried or vulnerable when using online technology. • 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 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, 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 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 ensure that any digital communications about pupils should be approved by parents. Should they have any concerns about their children to consult with the school instead of putting on a social media site. • to read, understand and promote the school Pupil Acceptable Use Agreement with their children • to access the school website /on-line student programmes / 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.
Wider school Community	• Any external individual / organisation will sign an Acceptable Use Policy prior to using any equipment or the Internet within school • •Take responsibility for the security of data. • •Develop an awareness of e-safety issues, and how they relate to pupils in their care. • •Model good practice in using new and emerging technologies. • •Know when and how to escalate e-safety issues. • •Maintain a professional level of conduct in their personal use of technology, both within and outside school. • •Take responsibility for their professional development in this area.

Communication:

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

- Policy to be posted on the school website and network
- Policy to be part of school induction pack for new staff
- Acceptable use agreements discussed with pupils at the start of each year.
- Acceptable use agreements to be issued to whole school community, usually on entry to the school
- Acceptable use agreements to be held in pupil and personnel files

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/ teachers/Phase-leader / Online Safety Coordinator / Headteacher;
  - informing parents or carers;
  - removal of Internet or computer access for a period, [which could ultimately prevent access to files held on the system, including examination coursework];
  - referral to LA / Police.

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

- Complaints of online 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 and Monitoring

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

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

2. Education and Curriculum

Pupil Online safety curriculum

This school

- Has a clear, progressive Online safety education programme as part of the Computing curriculum / PSHE curriculum. It is built on LA / LGfL online safeguarding and online literacy framework for EYFS to Y6/ national guidance. 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 online bullying, sexting, extremism and trolling and know how to seek help if they are affected by any form of online bullying.
    - To know how to report any abuse including online 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 member, or an organisation such as ChildLine or the CLICK CEOP button.

- 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 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.
- 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 also 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 online; online gaming / gambling;

Staff and governor training
This school
- Ensures staff know how to send or receive sensitive and personal data and understand the requirement to encrypt data where the sensitivity requires data protection;

- Makes regular training available to staff on online safety issues and the school's online safety education program;<annual updates/

- 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 e-safeguarding policy and the school's Acceptable Use Policies.

Parent awareness and training

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

3. Expected Conduct and Incident management

Expected conduct
In this school, all users:
- o are responsible for using the school Computing 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.)
- o need to understand the importance of misuse or access to inappropriate materials and are aware of the consequences
- o need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- o should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online E-Safety Policy covers their actions out of school, if related to their membership of the school
- o 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 online bullying

Staff

- o are responsible for reading the school's Online E-safety policy and using the school Computing systems accordingly, including the use of mobile phones, and hand held devices.

Students/Pupils
- o should have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations

Parents/Carers
- o should provide consent for pupils to use the Internet, as well as other technologies, as part of the Online E-safety acceptable use agreement form at time of their child's entry to the school
- o should know and understand what the 'rules of appropriate use' are and what sanctions result from misuse

Incident Management
In this school:
- o 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
- o 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.
- o support is actively sought from other agencies as needed (e.g. the local authority and regional broadband grid, UK Safer Internet Centre helpline) in dealing with online safety issues
- o monitoring and reporting of online 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
- o parents / carers are specifically informed of online safety incidents involving young people for whom they are responsible.
- o 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 IT and Computing infrastructure

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

This school:
- o Has the educational filtered secure broadband connectivity through the LGfL and so connects to the 'private' National Education Network;
- o 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;
- o Uses USO user-level filtering where relevant, thereby closing down or opening up options appropriate to the age / stage of the students;

- o 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;

- o Uses DfE, LA or LGfL approved systems such as S2S, USO FX, secured email to send personal data over the Internet and uses encrypted devices or secure remote access were staff need to access personal level data off-site;

- o Blocks all Chat rooms and social networking sites except those that are part of an educational network

- o Only unblocks other external social networking sites for specific purposes / Internet Literacy lessons;

- o 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;

- o Uses security time-outs on Internet access where practicable / useful;

- o Works in partnership with the LGfL to ensure any concerns about the system are communicated so that systems remain robust and protect students;

- o 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;

- o Ensures all staff and students have signed an acceptable use agreement form and understands that they must report any concerns;

- o Ensures pupils only publish within an appropriately secure environment: the school's learning environment/ the London LEARNING PLATFORM/ LGfL secure platforms such as J2Bloggy, etc.

- o Requires staff to preview websites before use [where not previously viewed or cached] and encourages use of the school's Learning Platform as a key way to direct students to age / subject appropriate web sites; Plans the curriculum context for Internet use to match pupils' ability, using child-friendly search engines where more open Internet searching is required; e.g. yahoo for kids or ask for kids , Google Safe Search , …..

- o Never allows / Is vigilant when conducting 'raw' image search with pupils e.g. Google image search;

- o Informs all users that Internet use is monitored;

- o Informs staff and students that that they must report any failure of the filtering systems directly to the [*system administrator / teacher / person responsible for URL filtering*]. Our system administrator(s) logs or escalates as appropriate to the Technical service provider or LGfL Helpdesk as necessary;

- o 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;

- o Provides advice and information on reporting offensive materials, abuse/ bullying etc. available for pupils, staff and parents

- o Immediately refers any material we suspect is illegal to the appropriate authorities – Police – and the LA.

- **Network management (user access, backup)**
  This school
    o Uses individual, audited log-ins for all users - the London USO system;

    o Uses guest accounts occasionally for external or short term visitors for temporary access to appropriate services

    o *Uses teacher 'remote' management control tools for controlling workstations / viewing users / setting-up applications and Internet web sites, where useful;*

    o *Has additional local network auditing software installed;*

    o 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;

    o 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, this school:

- Ensures staff read and sign that they have understood the school's Online E-safety Policy. Following this, they are set-up with Internet, email access and network access. Online access to service is through a unique, audited username and password. We also *provide a different / use the same username and password* for access to our school's network;

- Staff access to the schools' management information system is controlled through a separate password for data security purposes;

- We provide pupils with an individual network log-in username. From Year 3 they are also expected to use a personal password for certain sites.

- All pupils have their own unique username and password which gives them access to the Internet, *and (for older pupils) their own school approved email account*;

- 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 do not switch the computers off during the day unless they are unlikely to be used again that day or have completely crashed. We request that they DO switch the computers off at the end of the day and we also automatically switch off all computers at 6 o'clock to save energy;

- 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 / 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;

- Makes clear responsibilities for the daily back up of MIS and finance systems and other important files;

- Has a clear disaster recovery system in place for critical data that includes a secure, remote back up of critical data, that complies with external Audit's requirements;

- Uses our broadband network for our CCTV system and have had set-up by approved partners;

- Uses the DfE secure s2s website for all CTF files sent to other schools;

- Ensures that all pupil level data or personal data sent over the Internet is encrypted or only sent within the approved secure system in our LA or through USO secure file exchange (USO FX);

- Follows ISP advice on Local Area and Wide Area security matters and firewalls and routers have been configured to prevent unauthorised use of our network;

- Our wireless network has been secured to industry standard Enterprise security level /appropriate standards suitable for educational use;

- All computer equipment is installed professionally and meets health and safety standards;

- Projectors are maintained so that the quality of presentation remains high;

- Reviews the school IT systems regularly with regard to health and safety and security.

Password policy

- This school makes it clear that staff and pupils must always keep their password and class passwords private, must not share it with others and must not leave it where others can find it;

- All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password private.

- We require staff to use <STRONG passwords for access into our Integris system.

- We require staff to change their passwords into the Integris, LGfL USO admin site, other secure system, every 90 days / twice a year.

E-mail

This school

- Provides staff with an email account for their professional use, *London Staffmail / LA email* and makes clear personal email should be through a separate account;

- Provides *highly restricted (Safe mail) / simulated environments for e-mail with Key Stage 1 pupils*; Uses Londonmail with students as this has email content control. Only year 5 &6 have access to this account.

- Does not publish personal e-mail addresses of pupils or staff on the school website.

- Will contact the Police if one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law.

- Will ensure that email accounts are maintained and up to date

- Reports messages relating to or in support of illegal activities to the relevant Authority and if necessary to the Police.

- Knows that spam, phishing and virus attachments can make e mails dangerous. We use a number of LGfL-provided technologies to help protect users and systems in the school, including desktop anti-virus product 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 taught about the online safety and 'netiquette' of using e-mail, blogging, any sites which encourage communication both in school and at home i.e. they are taught:
  - not to give out their contact details 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;
  - 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;

- o that they should think carefully before sending any attachments;
- o that they must immediately tell a teacher / responsible adult if they receive a communication which makes them feel uncomfortable, is offensive or bullying in nature;
- o not to respond to malicious or threatening messages;
- o not to delete malicious of threatening communication, but to keep them as evidence of bullying;
- o not to arrange to meet anyone they meet through communication without having discussed with an adult and taking a responsible adult with them;

- 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':

  - o the sending of multiple or large attachments should be limited, and may also be restricted by the provider of the service being used;
  - o the sending of chain letters is not permitted;
  - o embedding adverts is not allowed;

- All staff sign our LA / school Agreement Form AUP to say they have read and understood the e-safety rules, including e-mail and we explain how any inappropriate use will be dealt with.

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

- o Uploading of information is restricted to our website authorisers: is Office Manager

- o The school web site complies with the [statutory DfE guidelines for publications](#);

- o 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;

- o 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;

- o Photographs published on the web do not have full names attached;
- o We do not use pupils' names when saving images in the file names or in the tags when publishing to the school website;
- o We do not use embedded geodata in respect of stored images
- o We expect teachers using' school approved blogs or wikis to password protect them and run from the school website.
- o

Social networking

- o Teachers are instructed not to run social network spaces for student use on a personal basis or to open up their own spaces to their students, but to use the schools' preferred system for such communications.
- o The school's preferred system for social networking (twitter) will be maintained in adherence with the communications policy.

School staff will ensure that in private use:
- No reference should be made in social media to students / pupils, parents / carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the *school* or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Video Conferencing
This school
- o Only uses the LGfL / Janet supported services for video conferencing activity;
- o Only uses approved or checked webcam sites;

CCTV

- o We have CCTV in the school as part of our site surveillance for staff and student safety. We will not reveal any recordings (*retained by the Support Provider for 28 days*), without permission except where disclosed to the Police as part of a criminal investigation.
- o 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 .Equipment and Digital Content
Ipads operate separately from the core school network.

Personal mobile phones and mobile devices
- 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.
- Student mobile phones are discouraged. 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 or students need to contact each other during the school day, they should do so only through the School's telephone. Staff may use their phones during break times.

Staff use of personal devices
- Staff handheld devices, including mobile phones and personal cameras must be noted in school – name, make & model, serial number. Any permitted images or files taken in school must be downloaded from the device and deleted in school before the end of the day.

- 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 students, parents or carers is required.

- 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.

- Staff should not use personally-owned devices, such as mobile phones or cameras, to take photos or videos of students and will only use work-provided equipment for this purpose.

- If a member of staff breaches the school policy then disciplinary action may be taken.

- Where staff members are required to use a mobile phone for school duties, for instance in case of emergency during off-site activities, or for contacting students or parents, then a school mobile phone will be provided and used. In an emergency where a staff member doesn't have access to a school-owned device, they should use their own device and hide (by inputting 141) their own mobile number for confidentiality purposes.

Digital images and video
In this school:

- We gain parental / carer permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter / son joins the school;

- We do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials / DVDs;

- Staff sign the school's Acceptable Use Policy and this includes a clause on the use of mobile phones / personal equipment for taking pictures of pupils;

- If specific pupil photos (not group photos) are used on the school web site, in the prospectus or in other high profile publications the school will obtain individual parental or pupil permission for its long term use

- The school blocks/filter access to social networking sites or newsgroups unless there is a specific approved educational purpose;

- Pupils are taught about how images can be manipulated in their e-safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children as part of their IT 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.

Data security: Management Information System access and Data transfer

See data security policy

Asset Tracking and disposal

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

Appendices:
1.   Acceptable Use Agreement (Staff)
2.   Acceptable Use Agreement (Pupils)
3.   Acceptable Use Agreement including photo/video permission (Parents)
4.   Protocol for responding to Online safety incidents

http://www.lgfl.net/esafety/Pages/policies-acceptable-use.aspx - handling infringements.
http://www.digitallyconfident.org/images/resources/first-line-information-support-HQ.pdf - page 23 onwards.

5.   Protocol for Data Security- see data protection policy
6.   Search and Confiscation guidance from DfE
https://www.gov.uk/government/publications/searching-screening-and-confiscation

Staff Acceptable Use Agreement

ICT and the related technologies such as email, the internet and mobile phones are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with Annie Ashraf- school e Safety coordinator.

- ➢ I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body.
- ➢ I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- ➢ I will ensure that all electronic communications with pupils and staff are compatible with my professional role
- ➢ I will only use the approved, secure email system(s) for any school business.
- ➢ I will ensure that personal data (such as data held on G2) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- ➢ I will not browse, download or upload material that could be considered offensive or illegal.
- ➢ I will not send to pupils or colleagues material that could be considered offensive or illegal
- ➢ Images of pupils will only be taken (including on camera phones) and used for professional purposes and will not be distributed outside the school network without the permission of the parent/ carer.
- ➢ I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Head teacher.
- ➢ I will respect copyright and intellectual property rights.
- ➢ I will support and promote the school's e-Safety policy and help pupils to be safe and responsible in their use of ICT and related technologies.
- ➢ I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to the appropriate to the e-safety co-coordinator.
- ➢ I will not connect a computer, laptop or other device (including USB flash drive), to the network / Internet that does not have up-to-date anti-virus software, and I will keep any 'loaned' equipment up-to-date, using the school's recommended system.
- ➢ While teacher laptops is on loan I will take full responsibility for its security and safely and not leave it unattended at any time. Loss, theft or damage should be reported to the school as soon as possible.
- ➢ I will also take full responsibility for the security of the any ICT resource (laptops, cameras, ipads). Loss, theft or damage should be reported to the school as soon as possible. Please do not lend any of these resources to anyone outside your year group. Please not if an ICT resource is lost, the school may charge you for replacing this.

- I will ensure that any private social networking sites / blogs etc that I create or actively contribute too are not confused with my professional role and appropriate privacy settings put into place.
- I agree and accept that any laptop, usb stick, camera loaned to me by the school, is provided solely to support my professional responsibilities and that I will notify the school of any "significant personal use" as defined by HM Revenue & Customs.

User Signature

I agree to follow this code of conduct and to support the safe use of ICT throughout the school

Laptop: Model
         Make
         Security Tag
         Haringey Security Tag

Ipad
Security Tag
Haringey Security Tag

Signature …………………………………… Date ……………………

Full Name ……………………………………..(printed)

Job title . . . .
……..

Key Stage 2 Pupils e-safety agreement

For my own personal safety – everywhere!

I will ask permission from a member of staff before using the Internet at school.

I am aware of "stranger danger" when on line and will not agree to meet online friends.

I will tell an adult about anything online which makes me feel uncomfortable.

I will not try to bypass the system to reach websites the school has blocked.

I understand that the school may check my files and may monitor the web pages I visit.

When in school I will only contact people with my teacher's permission.

To keep the system safe

I will only use my own login and password, which I will keep secret.

I will not access other people's files.

I will not play games on a school computer unless my teacher has given me permission.

I will not install software on school computers.

I will not use the system for gaming, gambling, shopping, or uploading videos or music.

I will be very careful when sharing pictures or video of myself or my friends.

If I am in school, I will always check with a teacher.

I will not put my "Personal Information" online. (My full name, birthday, phone number, address, postcode, school etc.)

Responsibility to others

The messages I send will be polite and responsible.

I will not upload images or video of other people without their permission.

Where work is copyrighted (including music, videos and images,) I will not either download or share with others. I will always quote the source of any information gained from the Internet i.e. the web address, in the documents I produce.

I understand that the school may take action against me if I am involved in inappropriate

behaviour on the internet and mobile devices.

I will avoid any acts of vandalism. This includes, but is not limited to, uploading or creating computer viruses and mischievously deleting or altering data from its place of storage.

I understand that if I don't follow these rules, my access to the school computer, ipads, network system/Internet/Email may be suspended, and my parents/carers will be informed

Personal Devices

It is not permitted for pupils to use Mobile Phones during the school day.

Other devices (e.g. Games consoles, cameras) should not be brought into school, unless my teacher has given me permission. The school cannot accept responsibility for loss or damage to personal devices.

Pupil name: _____   Class_____

☐ **I have read the school 'rules for E-safety'.   My teacher has explained them to me.**

☐ **I understand these rules are there to help keep me safe, and my friends and family safe.   I agree to follow the rules.**

☐ **This means I will use the computers, ipads, Internet, e-mail, online communities, digital cameras, video recorders, and other ICT in a safe and responsible way.**

☐ **I understand that the school can check my computer files, and the Internet sites I visit, and that if they have concerns about my safety, that they may contact my parent / carer.**

Pupil's signature _____Date: ___/___/___

Please send a signed copy home for parents.

Pupil Information Form Completed by Parents when they join the school.

Photographs
 	
Your child is likely to be photographed or filmed while engaging in the curriculum at Tetherdown. These photos or films may be subsequently used for display purposes, in publications such as our newsletter or on our website. Very occasionally they may be published externally, eg newspapers. We take care to ensure as far as possible that names are not attributable to individuals.
 	
1. I give permission for my child to be photographed/filmed at school for:-
   a. Internal use (eg displays)
   b. Publications (eg newsletter and website)
   c. External publications (eg newspaper)
	☐ Yes
	☐ Yes
	☐ Yes
		☐ No
		☐ No
		☐ No

E-Safety As part of the school's ICT curriculum we offer pupils supervised access to an educationally filtered internet service and restricted access e-mail. Further details of our e-safety policy is available on our website. 1. I give permission for my child to have access to and use the Internet, blogging, e-mail and other ICT facilities at school. 2. I understand that my child in Middle and Upper Phase (Y2-6) will also sign an e-safety agreement form and that their teacher will discuss responsible ICT use (introduced over several e-safety lessons).	☐ Yes ☐ Yes	☐ No ☐ No
Use of digital images, photography and video 1. I understand the school has a clear policy on 'the use of digital images and video' and I support this. 2. I understand that the school will necessarily use photographs of my child or include them in video material to support learning activities.	☐ Yes ☐ Yes	☐ No ☐ No
Social networking and media sites 1. I understand that the school has a clear policy on 'The use of social networking and media sites' and I support this. 2. I understand that children are not allowed to bring mobile phones into school. 3. I understand that the school takes any inappropriate behaviour seriously and will respond to observed or reported inappropriate or unsafe behaviour. 4. I will support the school by promoting safe use of the internet and digital technology at home and I will inform the school if I have any concerns. 5. I understand that I will not take and then share online, photographs of other children (or staff) at school events without permission.	☐ Yes ☐ Yes ☐ Yes ☐ Yes ☐ Yes	☐ No ☐ No ☐ No ☐ No ☐ No

Guidance: What do we do if?

An inappropriate website is accessed unintentionally in school by a teacher or child.

1. Play the situation down; don't make it into a drama.
2. Report to the head teacher/e- safety officer and decide whether to inform parents of any children who viewed the site.
3. Inform the school technicians and ensure the site is filtered (LGfL schools report to: Atomwide via the LGFL Helpdesk).
4. Inform the LA if the filtering service is provided via an LA/RBC.

An inappropriate website is accessed intentionally by a child.
1. Refer to the acceptable use policy that was signed by the child, and apply agreed sanctions.
2. Notify the parents of the child.
3. Inform the school technicians and ensure the site is filtered if need be.
4. Inform the LA if the filtering service is provided via an LA/RBC.

An inappropriate website is accessed intentionally by a staff member.
1. Ensure all evidence is stored and logged
2. Refer to the acceptable use and staffing policy that was signed by the staff member, and apply disciplinary procedure.
3. Notify governing body.
4. Inform the school technicians and ensure the site is filtered if need be.
5. Inform the LA if the filtering service is provided via an LA/RBC.
6. In an extreme case where the material is of an illegal nature:
a. Contact the local police and follow their advice.

An adult uses School IT equipment inappropriately.
1. Ensure you have a colleague with you, do not view the misuse alone.
2. Report the misuse immediately to the head teacher (or named proxy) and ensure that there is no further access to the device. Record all actions taken.
3. If the material is offensive but not illegal, the head teacher should then:
☐ Remove the device to a secure place.
☐ Instigate an audit of all ICT equipment by the schools ICT managed service providers or technical teams to ensure there is no risk of pupils accessing inappropriate materials in the school.
☐ Identify the precise details of the material.
☐ Take appropriate disciplinary action (undertaken by Headteacher).
☐ Inform governors of the incident.
4. In an extreme case where the material is of an illegal nature:
☐ Contact the local police and follow their advice.
☐ If requested to remove the device to a secure place and document what you have done.

All of the above incidences must be reported immediately to the head teacher and e-safety officer.

A bullying incident directed at a child occurs through email or mobile phone technology, either inside or outside of school time.
1. Advise the child not to respond to the message.
2. Refer to relevant policies including e-safety anti-bullying and PHSE and apply appropriate sanctions.
3. Secure and preserve any evidence through screenshots and printouts.

4.   Inform the sender's e-mail service provider if known.
5.   Notify parents of all the children involved.
6.   Consider delivering a parent workshop for the school community.
7.   Inform the police if necessary.
8.   Inform other agencies if required (LA, Child protection, LGFL)

Malicious or threatening comments are posted on an Internet site (such as social networking) about member of the school community (including pupils and staff).

1.   Inform and request the comments be removed if the site is administered externally.
2.   Secure and preserve any evidence.
3.   Send all the evidence to CEOP at ww.ceop.gov.uk/contact_us.html.
4.   Endeavour to trace the origin and inform police as appropriate.
5.   Inform LA and other agencies (child protection, Governing body etc).

The school may wish to consider delivering a parent workshop for the school community

You are concerned that a child's safety is at risk because you suspect someone is using communication technologies (such as social networking sites or gaming) to make inappropriate contact with the child

1.   Report to and discuss with the named child protection officer in school and contact parents.
2.   Advise the child on how to terminate the communication and save all evidence.
3.   Contact CEOP http://www.ceop.gov.uk/
4.   Consider the involvement police and social services.
5.   Inform LA and other agencies.
6. Consider delivering a parent workshop for the school community.

You are concerned that a child's safety is at risk because you suspect they are playing computer games that are inappropriate or certificated beyond the age of the the child

1.   Report to and discuss with the named child protection officer in school and contact parents.
2.   Advise the child and parents on appropriate games and content. You may want to use LGFL template letters to inform all or targeted parents.
3.   If the game is played within school environment, ensure that the technical team block access to the game
4.   Consider the involvement social services and child protection agencies.
5. Consider delivering a parent workshop for the school community.

You are aware of social network posts and pages created by parents about the school. While no inaccurate information is posted, it is inflammatory and disruptive and staff are finding it hard not to respond.

1.   Contact the poster or page creator and discuss the issues in person
2.   Provide central staff training and discuss as a staff how to behave when finding such posts and appropriate responses.
3.   Contact governing body and parent association
4.   Consider delivering a parent workshop for the school community.

All of the above incidences must be reported immediately to the head teacher and e-safety officer.

Children should be confident in a no-blame culture when it comes to reporting inappropriate incidents involving the internet or mobile technology: they must be able to do this without fear.