COLEGRAVE
PRIMARY SCHOOL

Computing & IT Policy

Irfan Amin
Computing & IT Leader

Updated: March 2017

Loving Learning,
Striving for Success,
Achieving Everyday

RIGHTS RESPECTING SCHOOLS
unicef
UNITED KINGDOM
LEVEL 1

Contents

Introduction

The purpose of this policy is to:

- Set out the key principles expected of all members of the school community at Colegrave Primary School with respect to the delivery of Computing, Online Safety and use of IT-based technologies.
- Safeguard and protect the children and staff of Colegrave Primary School.
- Assist staff 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.
- Outline the technical and strategic considerations made for the safe use of IT resources and facilities.
- Highlight the procedures to be used for dealing with incidents and concerns relating to IT.
- 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 staff who work with pupils.

What is Computing & IT?

Broadly speaking, the National Curriculum subject of Computing teaches pupils: how digital systems work, how they are designed and programmed, and the fundamental principles of information and computation. It also equips pupils to apply Information Technology to create products and solutions.

IT (Information Technology) is the technology that supports teaching and learning across the curriculum, including Computing. This includes the use of:

- Computers & Laptops
- Tablets
- Storage Devices and Media
- Mobile Phones
- Digital Cameras
- Digital Video Cameras
- Printers
- Scanners
- Audio Recording Devices
- Microphones
- Electronic Musical Instruments
- Sound Mixing Equipment/Software
- Programmable Toys
- Data Logging Equipment
- Augmented Reality Equipment/Software
- Software
- Applications
- The Internet
- Interactive Whiteboards
- Visualizers
- Performance Equipment
- Interactive Presentation Technologies
- Access and Assistive Technologies

In this policy the term 'Computing' will be used to describe the curriculum subject that has replaced ICT (Information and Communication Technology) and the term 'IT' (Information Technology) will be used when describing technology used to support teaching and learning across the curriculum.

Our Vision

Our vision is to provide *outstanding* Computing teaching and learning opportunities that will empower pupils to use IT confidently and skilfully in the future. Through challenging and engaging lessons, our pupils will become passionate about technology in the classroom and at home. We are also committed to ensuring that pupils meet our high expectations and apply their learning in a variety of contexts. Above all we want to ensure our pupils are safe and respectful when engaging with technology at home and school, making good choices about their online conduct and contact with others.

Aims

At Colegrave Primary School we aim to:

- Make learning in Computing exciting, engaging and challenging for all pupils.
- Ensure all pupils have access to high-quality teaching and learning opportunities in Computing.
- Deliver a broad and cutting-edge Computing curriculum that provides a variety of contexts for using a range of IT skills, applications and equipment.
- Educate pupils about safe, responsible and respectful use of technology, the Internet and communication platforms, as well as, the limitations and consequences of its misuse.
- Use IT to support, extend and enhance teaching and learning in Computing and across the Primary Curriculum
- Facilitate the learning of pupils with Special Educational Needs and Disabilities (SEND) using IT and assistive technology.
- Promote the inclusion of learners with English as an Additional Language (EAL).
- Provide specific opportunities to extend learning and accelerate the potential of pupils who demonstrate an aptitude for Computing.
- Provide enrichment opportunities to pupil's who have an enthusiasm and appreciation for computer science and technology.
- Support the subject knowledge and skill development of our school community though INSET and opportunities for Continuing Professional Development (CPD).
- Work alongside other Newham schools in creating opportunities to share good practice and raise the standard of Computing provision across the borough – through our role as a lead school in the Network of Excellence.

Computing in the National Curriculum

Key Stage 1
By the end of Key Stage pupils should be taught to:

- Understand what algorithms are, how they are implemented as programs on digital devices, and that programs execute by following precise and unambiguous instructions.
- Create and debug simple programs.
- Use logical reasoning to predict the behaviour of simple programs.
- Use technology purposefully to create, organise, store, manipulate and retrieve digital content.
- Recognise common uses of information technology beyond school.
- Use technology safely and respectfully, keeping personal information private; identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies.

Key Stage 2
By the end of Key Stage 2 pupils should be taught to:

- Design and write programs that accomplish specific goals, including controlling or simulating physical systems; solve problems by decomposing them into smaller parts.
- Use sequence, selection, and repetition in programs; work with variables and various forms of input and output; generate appropriate inputs and predicted outputs to test programs.
- Use logical reasoning to explain how a simple algorithm works and to detect and correct errors in algorithms and programs.
- Understand computer networks including the Internet; how they can provide multiple services, such as the World Wide Web; and the opportunities they offer for communication and collaboration.

- Describe how internet search engines find and store data; use search engines effectively; be discerning in evaluating digital content; respect individuals and intellectual property; use technology responsibly, securely and safely.

- Select, use and combine a variety of software (including internet services) on a range of digital devices to accomplish given goals, including collecting, analysing, evaluating and presenting data and information.

Within the National Curriculum programme of study, it is clear that there are three main aspects of the Computing curriculum:

- Computer Science
- Information Technology
- Digital literacy

	Key Stage 1	Key Stage 2
Computer Science	Understand what algorithms are; how they are implemented as programs on digital devices; and that programs execute by following precise and unambiguous instructions Create and debug simple programs Use logical reasoning to predict the behaviour of simple programs	Design, write and debug programs that accomplish specific goals, including controlling or simulating physical systems; solve problems by decomposing them into smaller parts Use sequence, selection, and repetition in programs; work with variables and various forms of input and output Use logical reasoning to explain how some simple algorithms work and to detect and correct errors in algorithms and programs Understand computer networks including the internet; how they can provide multiple services, such as the World Wide Web Appreciate how [search] results are selected and ranked
Information Technology	Use technology purposefully to create, organise, store, manipulate and retrieve digital content	Use search technologies effectively Select, use and combine a variety of software (including internet services) on a range of digital devices to design and create a range of programs, systems and content that accomplish given goals, including collecting, analysing, evaluating and presenting data and information
Digital Literacy	Recognise common uses of information technology beyond school Use technology safely and respectfully, keeping personal information private; identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies	Understand the opportunities [networks] offer for communication and collaboration Be discerning in evaluating digital content Use technology safely, respectfully and responsibly; recognise acceptable/unacceptable behaviour; identify a range of ways to report concerns about content and contact

Teaching & Learning

Computing lessons are usually 1½ hours in duration, taking place in classrooms using mobile devices such as iPads, Laptops or Chromebooks. Whenever possible, we encourage 'unplugged' lessons or activities in addition to hands-on learning. Teaching in Computing should also promote the development of computational thinking skills as well as independence, interdependence, creativity and problem solving skills.

It is the expectation that Computing is taught in units as a series of 5-6 lessons, every afternoon in each half-term. It is expected that Online Safety is taught over 5 'flexible' lessons, throughout the year. Where possible lessons should link to a topic or relevant theme, in order to apply what is being taught across the curriculum and vice versa.

Each year group uses Core Computing Objectives and Assessment (CoCOA) document devised by The Digital Curriculum to determine what pupils will be learning. This document clearly defines the units and learning objectives for every Computing and Online Safety lesson pupils will be taught.

The main responsibility of the Computing & IT Leader is to collaborate with Teachers to plan and deliver 'Good to Outstanding' Computing Lessons. This includes supporting planning and resourcing as well as, team-teaching and providing individualised training. The Year Leader is responsible for coordinating adequate time for planning, preparing and training in advance of the lessons with the Computing & IT Leader.

Assessment

The Computing Progression Pathways is fast becoming the national standard for interpreting the breath and depth of the Computing curriculum in schools. The purpose of the Progression Pathways framework is to support teachers assessing pupil progress in Computing. It was devised by Mark Dorling and Computing At School based on the 2014 National Curriculum for Computing areas of study.

From September 2015 the Core Computing Objectives and Assessment (CoCOA) all pupils are taught throughout the year will be linked to the Computing Progression Pathways framework. This will allow Teachers to identify the progress pupils are making in Computing against a national standardised framework.

Examples of work are kept in the Digital Learning Portfolios as a 'snapshot' of what pupils have been learning in Computing and also the ways they have been using IT across the curriculum. In these portfolios photocopied and annotated examples of three pupils work are kept and monitored each term.

Resources

As part of our whole-school vision for teaching and learning, we strongly believe that technology should be fully integrated within the classroom. At Colegrave Primary School we aim to provide pupils range of technology to facilitate learning and IT skills – preparing pupils for the future.

Each classroom is equipped with a PC, laser printer and an interactive whiteboard for general teaching use. All classrooms have access to both individual and shared Wi-Fi Access Points, to enable Internet access on mobile and portable devices.

Each class has access to Apple iPad Minis (stored in shared charging trolleys) for pupil use. iPads enable pupils to instantly access the Internet, interact with applications and instantly create. The number of iPads available is as follows:

- 5 in Reception per class (1:6 ratio)
- 10 in Key Stage 1 per class (1:3 ratio)
- 15 in Key Stage 2 per class (1:2 ratio)

In Key Stage 2 there is also access to 30 Google Chromebooks for access to more conventional applications such as word processing, spreadsheets, presentations and unparalleled access to the Internet and cloud-based applications.

In addition to mobile technology, we have a range of IT resources, available for use, including:

- Voice Recorders
- DSLR Camera
- HD Video Cameras
- Music Production equipment
- Headphones
- Microphones
- Programmable Toys
- Chroma Key (Green Screen) equipment
- Video Games
- Interactive Games
- Electronics kits
- Invention Kits
- Reference Books

Monitoring & Review

At Colegrave Primary School, we rigorously review our performance, procedures and systems to ensure our Computing and IT provision remains exceptional. The opportunities for monitoring and review include:

- Examples of work are monitored at the end of each half term, to observe the standard, breadth and continuity of learning in Computing across the school. The findings are then presented to the Senior Leadership Team.

- A sample of Online Safety work is scrutinised each half term to gain an insight into the effectiveness of Online Safety sessions and to identify misconceptions in teaching.

- Meetings are held every half term between the Computing & IT Leader and Headteacher to update on actions taken towards the strategic improvement of Computing & IT.

- A strategic self-review is carried out in April to support school improvement in Computing & IT across the school. This is based upon the Self-Review Framework from NAACE. In May the findings of this review are then used to generate actions to be taken in the next academic year.

- An Online Safety review is carried out in June, in conjunction with the Safeguarding Leader to identify the effectiveness of Online Safety procedures. This is based upon the Self-Review materials from 360° Safe.

- The Computing & IT policy is reviewed in July each year. This will then be revised and submitted for approval by the Governing Body in September.

Incident Management

- There is strict monitoring and application of this 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.

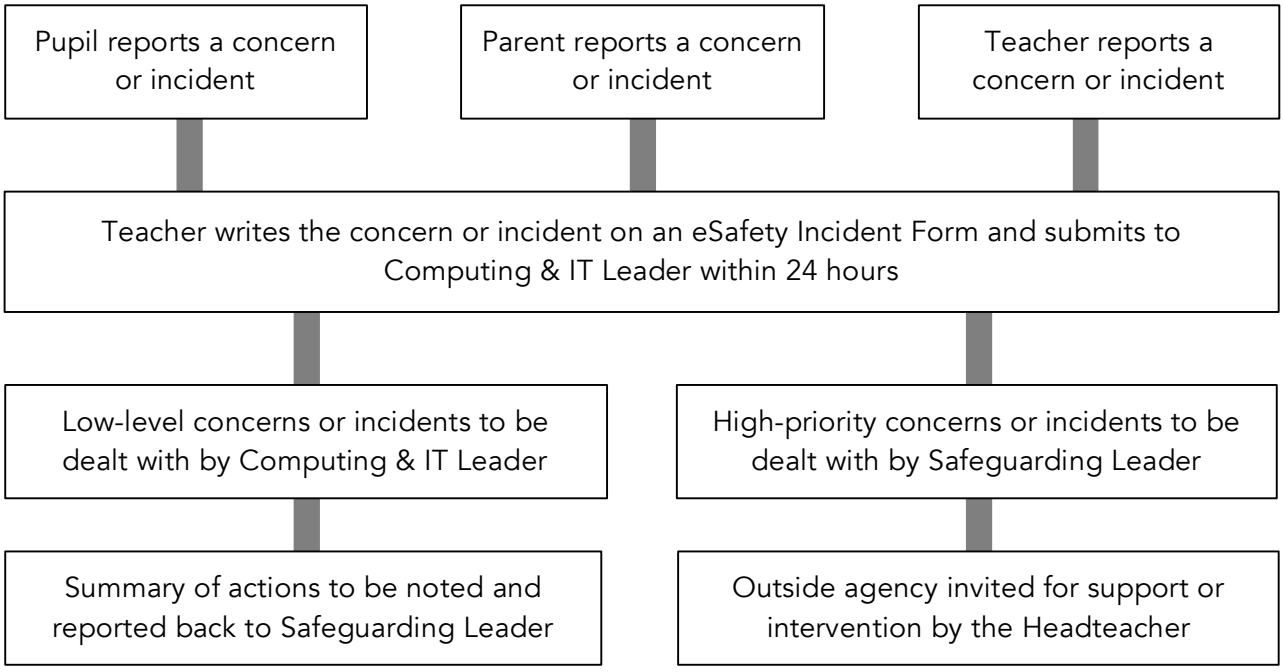
- All members and its wider community are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through our school's incident management processes.

- Support is actively sought from other agencies as needed (e.g. LGfL, Local Authority, Safer Internet Centre helpline, Police) in dealing with Online Safety / eSafeguarding issues.

- 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 by the: Computing & IT Leader, Safeguarding Officer, Headteacher and Governing Body.

- Parents/Carers are specifically informed of Online Safety incidents involving young people for whom they are responsible.

- We will contact the Police if our staff or pupils receive online communication that we consider is particularly disturbing or breaks the law.



Online Safety

At Colegrave, we understand the importance of educating pupils, parents and staff about safe and respectful online behaviour and conduct, protecting them from the following risks:

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
- Radicalisation
- Cyberbullying in all forms
- Identity theft (including 'frape', meaning to hack 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)
- Copyright (little care or consideration for intellectual property and ownership – such as music and film)

All pupils in Years 1 to 6 are expected to learn about a different aspect of Online Safety each half term. Each of these sessions will be between 2 to 3 hours and will follow the whole-school scheme of work developed by The Digital Curriculum.

For each unit pupils will be given a booklet containing all the relevant teaching points alongside assessment questions for checking their understanding. Teachers will be expected to use these booklets to plan high-quality learning opportunities through interactive activities, discussion and group work – with a focus on exploring issues raised and ensuring pupils are equipped to make positive choices.

In addition to this, we also celebrate Safer Internet Day each year (in February) by organising activities and workshops for all pupils.

Internet Access

We have taken the following measures for controlling Internet Access, security, virus protection and web filtering. To ensure the Internet and online services are used safely, Colegrave Primary School:

- Has the educational filtered secure broadband connectivity through the LGfL and so connects to the 'private' National Education Network.
- Uses the LGfL Net Sweeper filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature, etc.
- All changes to the filtering policy are logged and only available 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 of the pupils.
- Ensures network health through use of Sophos Anti-Virus software (from LGfL) and network set-up so staff and pupils cannot download executable files.
- 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.
- Blocks all chat rooms and social networking sites except those that are part of an educational network.
- Only unblocks other external social networking sites for specific purposes (such as Online Safety lessons).
- Has blocked pupil access to music download or shopping sites – except those approved for educational purposes at a regional or national level.
- Uses security time-outs on Internet access where applicable.
- Works in partnership with 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 when encouraging pupils to use mobile technology.

- Ensures all staff and students have signed an Acceptable Use Agreement and understands that they must report any concerns.

- Ensures pupils only publish within an appropriately secure environment.

- Requires staff to approve websites before use where not previously viewed or cached.
- Requires staff to plans the curriculum context for Internet use to match pupils' ability, using Google Safe Search.

- Never allows 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 Computing & IT Leader. Here reports will be logged and escalates as appropriate to School-Based Technician or LGfL Helpdesk as necessary.

- Makes clear all users know and understand what the 'rules of appropriate use' are and what sanctions result from misuse – through staff meetings and teaching programme.

- Provides advice to pupils, staff and parents and information on reporting offensive materials, abuse and bullying etc.

- Immediately refers any material we suspect is illegal to the appropriate authorities.

School Network

We have taken the following measures for managing and securing network resources. To ensure the network is used safely, Colegrave Primary School:

- Uses individual, audited log-ins for all users - the London USO system.
- Uses guest accounts occasionally for external or short term visitors for temporary access to appropriate services.
- Uses RM CC4 as a management control tools for controlling workstations, viewing users, setting-up applications and Internet web sites.
- Ensures the Computing & IT Leader is up-to-date with LGfL services and policies and requires the School-Based Technician to be up-to-date with LGfL services and policies.
- Storage of all data within the school will conform to the UK data protection requirement.
- 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.
- Ensures staff read and sign that they have understood the school's Online Safety Policy. Following this, they are setup with Internet, email access and network access. Online access to service is through a unique, audited username and password.
- We also 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 login username.
- All pupils have their own unique username and password which gives them access to the Internet, the Learning Platform and for pupils in Years 4, 5 and 6, 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 logon or use generic or staff logins as these have far less security restrictions and inappropriate use could damage files or the network.

- Has setup 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.

- Request that pupils and staff switch off computers and devices at the end of the day and we also automatically switch off all computers at 7pm 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.

- 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.

- Maintains equipment to ensure Health and Safety is followed (e.g. equipment installed and maintained by School-Based Technician).

- 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 RAV3 system.

- Does not allow any outside Agencies or parents to access our network remotely except where there is a clear professional need and then access is restricted and is only through approved systems.

- Provides pupils and staff with access to content and resources through the approved Learning Platform which staff and pupils access using their username and password (their USO username and password).

- Makes clear responsibilities for the daily backup 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.

- 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 appropriate standards suitable for educational use.

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

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

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

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

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

- We require staff to use 'strong' passwords for access into our MIS system.

- We require staff to change their passwords into the MIS, LGfL USO admin site every 90 days.

E-mail

At Colegrave we have taken the following measures to protect the staff and pupils while using e-mail facilities intended for school use:

School

- Provides staff with an LGfL StaffMail account for their professional use and makes clear this should not be used for personal use.
- Provides highly restricted LGfL LondonMail for use with students as this has email content control.
- Does not publish personal e-mail addresses of pupils or staff on the school website. We use anonymous or group e-mail addresses, such as *info@colegrave.newham.sch.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.
- 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.

Pupils

- We use LGfL LondonMail with pupils and lock this down where appropriate using LGfL SafeMail rules.
- Pupils' LGfL LondonMail e-mail accounts are intentionally anonymised for their protection.
- Pupils are introduced to, and use e-mail during Key Stage 2.
- Pupils can only receive external mail from, and send external mail to, addresses if the SafeMail rules have been set to allow this.

- Pupils are taught about the safety and 'netiquette' of using e-mail both in school and at home, including:
    - Not to give out their e-mail address unless it is part of a school managed project or to someone they know and trust and is approved by their teacher or parent/carer;
    - That an e-mail is a form of publishing where the message should be clear, short and concise;
    - That any e-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper;
    - They must not reveal private details of themselves or others in e-mail, such as address, telephone number etc.;
    - To 'Stop and Think Before They Click' and not open attachments unless sure the source is safe;
    - That they should think carefully before sending any attachments;
    - Embedding adverts is not allowed;
    - That they must immediately tell a trusted 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 Acceptable Use Agreement 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.

Continued…

Staff

- Staff only use 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 e-mail to transfer staff or pupil personal data. We use secure S2S (for school to school transfer); Collect; USO-FX or other approved LA system.
- Staff know that e-mail sent to an external organisation must be written carefully, 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 Acceptable Use Agreement 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.

Social Media

In addition to the school website, we also have a number of social media accounts we maintain which include:

- Twitter: for instant communication with parents following @colegraveschool
- YouTube: for hosting videos on our channel www.youtube.com/colegraveschool

School Website

The Colegrave School Website has become a place to: celebrate the achievements of our pupils and recognise the school's successes.

The website address is www.colegrave.newham.sch.uk

The purpose of our school website is:

1. To promote the school;
2. To provide information to parents and teachers, and the wider community;
3. To act as a communication channel between teachers, parents and pupils;
4. To improve pupil learning and celebrate achievements;
5. To raise standards in teaching and learning.

At Colegrave we take the following precautions to protect the staff and pupils on our school website and associated social media accounts:

- We will ensure that no pupil can be identified or contacted either via or as a result of using, the school website or associated social media.

- Adults' names will be published as their title and last name e.g. Mr Smith or Ms Brown.

- Pupil's names will be published as their first name only e.g. Joe or Jane.

- Any images of pupils will not be labelled with their names.

- Permission for the use of photos or videos will be obtained from parents or carers before any pupil's image is used. This is completed beforehand, when a pupil joins the school.

- Only first names and year group will be used to identify where work is published online.

- Pupils will only be shown in photos where they are suitably dressed.

- Personal details of pupils or staff such as home addresses, telephone numbers, personal e-mail addresses etc. will not be released via the website.

- Links to external websites will be checked thoroughly before inclusion on the school website. The sites will be checked for the suitability of their content for their intended audience.

- Any text written by pupils will be reviewed before inclusion to ensure that no personal details are accidentally included that could lead to the identification of the pupil e.g. membership of after school clubs.

- All content will be reviewed to ensure that it is in no way defamatory.

- Written work will be checked to ensure (as far as possible) that no copyright or intellectual property rights are infringed.

- Any dates or events happening within school may be published. Details of school trips will not be published prior to the event, but may be reported on subsequently.

- All written material will be checked for its suitability for its intended audience.

- Wherever possible, permission must be sought for use of content (e.g. photographs, images, maps etc.) created by others.

- Parents have the right to refuse permission for their child's work and/or image to be published on the site.

- Those wishing to exercise this right should express their wishes in writing to the Head Teacher, clearly stating whether they object to work, images, or both being published. Parents will be notified of this right by publication of this policy on an annual basis with an acknowledgement receipt attached.

- It is the responsibility of the Computing & IT Leader to update the website regularly as agreed by the Headteacher

- It is understood that Teachers and Subject Leaders should regularly contribute 'content' for use on the school website

- The school web site complies with the statutory The School Information (England) (Amendment) Regulations 2012.

NB: We have also purchased the domain www.colegrave.school exclusively for use with Google Apps for Education.

Data Protection

All staff must act and carry out its duty of care for the information assets it holds in line with its Data Protection Act 1998 commitments. At Colegrave Primary School, we take the following measures to ensure data is protected:

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

- The school has established an information-handling procedure and assessed the risks involved with handling and controlling access to all levels of information within school.

- The school has deployed appropriate technical controls to minimise the risk of data loss or breaches. At Colegrave Primary School this involves regular backups of both the administration and curriculum servers.

- All access to personal or sensitive information owned by the school will be controlled appropriately through technical and non-technical access controls. At Colegrave Primary School sensitive data is password-protected with access rights and privileges allocated to appropriate members of staff.

- All computers that are used to access sensitive information should be locked when unattended. Users should be vigilant when accessing sensitive or personal information on screen to ensure that no one else, who may be unauthorised, can read the information.

- All access to information systems should be controlled via a suitably complex password.

- All information on school servers shall be accessed through a controlled mechanism, with file permissions allocated and assessed on a need to know basis.

- Staff will not leave personal and sensitive printed documents on printers within public areas of the school.

- All physical information will be stored in controlled access areas.

- All communications involving personal or sensitive information (email, fax or post) should be appropriately secured.

- All personal and sensitive information taken offsite will be secured through appropriate technical controls, e.g. encrypted disk, and encrypted removable media, remote access over encrypted online portal.

- All devices taken off site, e.g. laptops, tablets, removable media or phones, will be secured in accordance with the school's information-handling procedures and, for example, not left in cars or insecure locations.

Data Security

Strategic and operational practices
At this school:

- The Head Teacher is the Senior Information Risk Officer (SIRO).
- 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 Capita SIMS.
- We ensure ALL the following school stakeholders sign an Acceptable Use Agreement form. We have a system so we know who has signed
    - Pupils
    - Teachers (including Trainees)
    - Parents
- We follow Local Authority (LA) guidelines for the transfer of any data, such as MIS data or reports of pupils, to professionals working in the LA 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 at least annual housekeeping to review, remove and destroy any digital materials and documents which need no longer be stored.

Technical Solutions
At this school:

- Staff have secure area(s) on the school network to store sensitive documents or photographs.

- We require staff to log-out of systems when leaving their computer, but also enforce system lockout after 10 minutes idle time.

- We will provide an encrypted flash drives if any member of staff has to take any sensitive information off site.

- We use the DfE S2S site to securely transfer CTF pupil data files to other schools.

- We use the Pan-London Admissions system (based on USO FX) to transfer admissions data.

- Staff with access to the Admissions system use LGfL OTP tags as an extra precaution.

- We use RAv3 with its 2-factor authentication for remote access into our systems.

- We use LGfL USO FX to transfer other data to schools in London, such as references, reports of pupils.

- We use the LGfL secure data transfer system, USO AutoUpdate, for creation of online user accounts for access to broadband services and the London content.

- We store any Protect and Restricted written material in locked storage areas within the school.

- DBS-checked staff from Newham Partnership Working (NPW) manage both the curriculum and admin servers (located in the server cupboard).

- We will begin to implement LGfL GridStore for backup and disaster recovery on our curriculum and admin servers.

- We comply with the WEEE directive on equipment disposal by using an approved or recommended disposal company for disposal of equipment where any protected or restricted data has been held and get a certificate of secure deletion for any server that once contained personal data.

- All-paper based sensitive information is shredded, using cross cut shredder located in the staff room.

Health & Safety

At Colegrave Primary School we follow Local Authority (LA) advice and ensure that our equipment is given annual Portable Appliance Testing (PAT) by an LA approved testing officer.

This is a legal requirement as set out in the Electricity at Work Regulations (1989).

IT resources should be treated with the same care as any other electrical equipment. It is the responsibility of staff to ensure there are no immediate hazards or safety risks from non-technical issues, which include:

- Preventing inherent risks from tripping on trailing wires.
- Ensuring food and drink are not placed near electrical equipment.
- Avoiding overheating of equipment due to prolonged and unsupervised use.
- Reporting of potential hazards and risks to either the Computing & IT Leader or the school's designated Health and Safety officer(s).
- Being responsible for the behaviour and conduct of pupils using IT equipment in their classrooms and around the school.
- Ensuring pupils do not use IT resources in an unsupervised capacity.
- Consulting the Computing & IT Leader or SENDCo with regard to any implications of the use of IT for known medical conditions (e.g. epilepsy, visual or physical impairment).
- Ensuring (where necessary) that pupils are given legally sufficient working conditions when using computers, with respect to: posture, seating, Repetitive Strain Injury (RSI) prevention, lighting and breaks.
- Following the manufacturer safety guidance for using digital projectors and interactive whiteboards.

Environmental Impact

At Colegrave Primary School, we take the following measures to reduce the environmental impact of out IT usage:

- Computers and mobile devices automatically switch off at 7pm to save energy.
- Waste paper is placed into collection bins in the photocopying area for recycling.
- Laser toner cartridges are collected for recycling by a 3rd party company.
- Batteries are collected and disposed of at local battery recycling facility.
- We encourage staff to 'think before you print' to reduce printing.
- We encourage staff to switch off computer monitors whenever they are left unattended.

Asset Disposal

Details of all school-owned hardware will be recorded in a hardware inventory.

All redundant equipment will be disposed of through an authorised agency. This will include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data.

All redundant equipment that may have held personal data will have the storage media forensically wiped. Alternatively, if the storage media has failed, it will be physically destroyed. The school will only use authorised companies who will supply a written guarantee that this will happen.

Disposal of any equipment will conform to The Waste Electrical and Electronic Equipment Regulations 2006 and/or The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007.

Further information can be found on the Environment Agency website.

Mobile Phone & Personal Devices

The possession and use of mobile phones and personal devices has become an important issue within schools. Therefore as a response to this, the following measures have been agreed on the use of mobile phones and personal devices:

- Mobile phones and personal devices brought into school by staff are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of mobile phones or personal devices brought into school.

- The theft of mobile phones or personal devices will be investigated by a Senior Leader. It is however at the discretion of the school to report the incident to the police for further investigation. Details of incidents of theft outside of school will be directly passed on to the Police.

- 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. 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. If a staff member is expecting a personal call they may leave their phone with the school office to answer on their behalf, or seek specific permissions to use their phone at other than their break times.

- Mobile phones and personal devices will not be used in any way during lessons or formal school time. They should be switched off or silent at all times.

- Pupils and staff are not permitted to take images or videos on mobile phones or personal devices of any member of the school community, except when express permission has been granted. Responsibility should be taken with regards to privacy, data protection and its use/intention.

- Mobile phones and personal devices are not permitted to be used in certain areas within the school site, e.g. changing rooms and toilets.

- Pupils and staff must not be given access to "CPS-CURRIC" Wi-Fi network under any circumstances for their mobile phone or personal devices. This network is reserved for 'static' school-based devices.

- Visitors with an LGfL USO may use the "GUEST" Wi-Fi network for Internet access on their mobile or personal devices. Visitors without an LGFL USO may request a member of staff to login on their behalf, ensuring their Internet usage is supervised.

- Pupils and staff must not use Personal devices (such as tablets) during lessons or formal school time unless as part of an approved or directed curriculum-based activity with consent from the Computing & IT Leader.

- Concerns raised by pupils regarding inappropriate communication and material sent using mobile messaging services (such as Facebook, WhatsApp and SnapChat) should be dealt with by the Phase Leader and Computing & IT Leader. Serious concerns should be referred to the Safeguarding Team and Headteacher, who will investigate further.

- The Computing & IT Leader, Safeguarding Team and Headteacher may confiscate mobile phones and personal devices with concerns relating to Online Safety and eSafeguarding. These parties have the right to check these devices without prior permission being granted from parents/carers in line with statutory guidance from the Government, in the: Screening, Searching and Confiscation (2014) document.

- Concerns relating to pupils and staff who use mobile phones or personal devices to access inappropriate, illegal or offensive material on school premises will be investigated by the Computing & IT Leader and Safeguarding Team.

- Parents/Carers or members of the public who raise concerns or allegations relating to mobile phone or personal devices belonging to or owned by pupils or staff, should be initially dealt with (and initially investigated) by the Computing & IT Leader. If these concerns or allegations deemed to be serious, the matter will be passed to the Safeguarding Team and/or the Headteacher.

Pupils

- The School strongly advises that student mobile phones should not be brought into school.

- The School accepts that there may be particular circumstances in which a parent wishes their child to have a mobile phone for their own safety.

- Pupils in Years 5 and 6 are only permitted to bring mobile phones to school if walking home unaccompanied (as agreed in the admission policy) for the purpose of contacting a responsible adult in an emergency situation.

- Pupils who have obtained consent must hand-in their mobile phones and personal devices to their Teacher during registration. These devices must be collected after-school. Pupils who wish to use them during school must first obtain permission from their Teacher before doing so.

- If a student breaches the school policy then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to parents or carers after the matter has been discussed with parents.

- If a student needs to contact his or her parents or carers, they will be allowed to use a school phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office.

- Pupils must not use mobile phones and personal devices in any way during lessons or formal school time.

- Pupils must switch off or silence their devices that all times while in the school premises.

- The Safeguarding Team will decide upon an appropriate course of action for pupils accessing 'highly inappropriate' content or material.

Staff

- Staff mobile phones and personal device information must be recorded in school. This information will include: name, make, model, serial number, MAC Address.

- Staff are permitted to use their mobile phones and personal devices during breaks and before or after school. Staff must refrain from using their mobile phones or personal devices in front of pupils or parents.

- Staff must switch off or silence their devices that all times while in the school premises

- Staff are not permitted to use their own mobile phones or personal devices for contacting pupils, young people or their families outside a professional capacity.

- Where staff members are required to use a mobile phone for school duties, for instance in case of emergency during off-site activities, or for contacting pupils or parents, then a school mobile phone will be provided and used.

- In an emergency where the staff member doesn't have access to a school owned mobile phone, they should use their own devices and hide their own mobile numbers for confidentiality purposes (by inputting 141 before the phone number).

- Staff may use the "STAFF" Wi-Fi network and pupils may use "GUEST" Wi-Fi network, using their LGfL USO username and password to login, for Internet access on their mobile or personal devices.

- Disciplinary action may be taken against staff who are in breech of this policy.

Social Networking

Social Networking is fast becoming the main platform for communicating and sharing content globally. The widespread availability and use of social networking brings opportunities to understand, engage and communicate with audiences in new ways. Social Networking platforms may include (but not limited to): Facebook, Flickr, Google+, Instagram, Pintrest, Skype, SnapChat, SoundCloud, Tumblr, Twitter and YouTube.

The following measures have been agreed, regarding social networking:

Pupils

- Pupils must not breach the Pupil Acceptable Use Agreement.

- Social Networking platforms such as Facebook, Twitter and Instagram are targeted at users aged 13 years or older and clearly state users must meet this requirement. Therefore we do not endorse or approve the use of these platforms for pupils. We believe that it is the responsibility of parents/guardians to supervise and restrict use of these platforms.

- It is the responsibility of Teachers to educate pupils about the risks and legal implications of being users of these platforms.

- Pupils are not permitted to use personal Social Networking platforms in school at anytime. Educational Social Networking platforms (such as Fronter and Google Classroom) may be used with permission from the Computing & IT Leader. However strict permissions and privileges should be enforced to prevent abuse of the system.

- Pupils are not permitted to use school devices to access personal Social Networking platforms at any time of the day. Designated time will be allocated to pupils to access Educational Social Networking platforms.

- Pupils who are known to have cyberbullied or harassed others using Social Networking platforms will be spoken to by their Teacher or Phase Leader. Where incidents continue or escalate into physical or verbal bullying on school premises, anti-bullying procedures will be followed. If this continues the Safeguarding Team may pass on information about the incidents to CEOP or Police for their involvement.

- Pupils who are solely being cyberbullied or harassed online or outside the school premises will be supported by pastoral support team. We will always attempt to mediate and provide guidance to pupils about conducting themselves online

appropriately. However, ultimately we believe it is the responsibility of parents/carers to supervise and restrict use of these platforms. As a school we support (where possible) pupils and parent/carers concerns, but we have little power to police the use of these platforms. Therefore, any on going concerns may be reported to CEOP or Police for their involvement.

- Concerns raised by pupils regarding inappropriate, illegal or disturbing material sent using Social Networking platforms should be dealt with by the Computing & IT Leader and Safeguarding Team. Serious concerns should be referred to the Safeguarding Team and Headteacher, who will investigate further, following safeguarding procedures.

Staff

- Staff are not permitted to visit personal Social Networking platforms in any way during lessons or formal school time. Staff may visit these on their mobile phones or personal devices before or after school, or at break times, but may not use school computers or Wi-Fi access to do so.

- Staff must not breach the Staff Acceptable Use Agreement.

- Staff must not publish or share content which may result in actions for defamation, discrimination, breaches of copyright, data protection or other claims for damages. This includes but is not limited to material of an illegal, sexual or offensive nature that may bring the school into 'disrepute'.

- Staff are not permitted to interact with any pupils in the school or ex-pupil under the age of 16 under any circumstances using personal Social Networking platforms. Staff may interact with pupils from the school on educational Social Networking platforms with permission from the Computing & IT Leader.

- Staff should be aware of that posting 'out-of-work' activity may cause potential embarrassment for the employer (namely the School) and therefore may ask staff to remove such material or in serious instances may take disciplinary action.

Digital Images & Video

At Colegrave Primary School, we take the following measures to protect pupils when using digital images and video of them in school, on the school website or on promotional or marketing materials:

- We gain permission from parents and carers for use of digital photographs or video involving their child as part of the Photographic Consent Form when their child 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 Usage Agreement and this includes a clause on the use of mobile phones / personal equipment for taking pictures of pupils.

- If specific photos are used on the school 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 Online 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 Computing study.

- 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 identity of others and their location, such as house number, street name or school. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.

Roles and Responsibilities

Role of the Computing & IT Leader
It is the role of the Computing Subject Leader to:

- Provide professional leadership and management of Computing & IT across the school
- Monitor standards ensuring high-quality teaching, effective use of resources and improved standards of learning and achievement in Computing
- Design an engaging and challenging Computing curriculum and Scheme of Work
- Review, monitor and evaluate the Computing Schemes of Work to ensure continuity and progression for all pupils;
- Monitor teaching, planning and learning outcomes within Computing
- Ensure the school uses IT, and the latest technologies, effectively for teaching, learning, communication and administrative purposes
- Evaluate Computing & IT provision against self-review frameworks
- Define and agree appropriate improvement targets and strategies
- Take day to day responsibility for Online Safety issues and has a leading role in establishing and reviewing the school Online Safety policy and documents
- Work with the Safeguarding Team to ensure staff, pupils and parents are fully informed and aware of how to keep themselves and others safe in the digital world
- Ensure that Online Safety education is rigorously embedded across all year groups
- Review and update the Computing & IT policy
- Develop and maintain the school website ensuring it meets Ofsted requirements and provides a comprehensive, positive and informative reflection of the school
- Enable teachers to achieve expertise in planning for and teaching in the Computing with support and by leading or providing high quality professional development opportunities
- Modelling and team-teaching Computing lessons and cross-curricular IT across Reception and Key Stage 1 and 2
- Develop opportunities for staff to use IT to support cross-curricular learning, and provide coaching and training to help teachers achieve this
- Provide high-quality, relevant training which meets the needs of Trainees, Parents, Carers and Governors
- Establish extra-curricular activities and targeted enrichment opportunities for pupils
- Provide clear feedback, good support and sound advice to staff
- Coordinate the School-Based Technician and external IT support
- To communicate regularly with SLT and the designated Governor to discuss current issues and review incident logs
- Ensure that an Online Safety incident log is kept up to date
- Be responsible for planning and purchasing resources
- Organise and manage resources efficiently so that teaching and learning is effectively supported

- Manage the Computing budget, in conjunction with the School Business Manager
- Maintain the Asset Register
- Keep up-to-date with developments and changes in Computing education and pedagogy and take responsibility for their own professional development
- Be aware of both local and national developments in IT
- Contribute to the appraisal of staff in Computing
- Undertake any other duties as designated by the Headteacher

Role of the School-Based Technician
It is the role of the School-Based Technician to:

- Be familiar with the use and support of Windows Server & RM Connect along with other network software and general hardware.
- Provide general maintenance and technical housekeeping of computer systems, interactive whiteboards and peripheral devices
- Maintain efficient working of computer systems
- Perform installations of simple peripheral devices
- Install software and applications
- Manage and maintain school e-mail accounts provided by LGfL
- Maintain an up-to-date inventory of computer equipment
- Maintain network user accounts including addition and deletion of users
- Ensure and maintain appropriate working conditions in computer suites, including routine cleaning of equipment
- Provide assistance, and where required, familiarisation training to teaching staff when using IT equipment
- Ensure anti-virus and security updates are kept current
- Provide additional services to schools as required such as:
    - Stock take of computer consumables and ordering
    - Replacing spent toners and cartridges for printers and refilling printers with paper
- Provide small group training sessions for staff for newly acquired equipment e.g. cameras, scanners etc.
- Maintain an up-to-date log of faults and remedial actions
- Build newly acquired and rebuild existing workstations as required
- Assist, where required, with simple tasks on the school admin network e.g. installing and sharing printers, the use of peripheral equipment and answering minor queries
- Assist, where required, with school Computing clubs where tasks are within the capabilities of the individual
- Report any Online Safety related issues that arises, to the Computing & IT Leader
- Carry out other duties that are in line with the purpose and grade of the job

Role of the Class Teachers

It is the role of the Class Teachers to:

- Plan opportunities for pupils to develop their subject knowledge and computational thinking skills in Computing lessons and IT skills across the curriculum
- Deliver good to outstanding Computing lessons or cross-curricular IT lessons
- Assess and provide feedback to pupils about their progress in Computing
- Liaise with the Computing & IT Leader for support with the planning, delivery and assessment of learning
- Embed Online Safety issues in all aspects of the curriculum and other school activities
- Supervise and guide pupils carefully when engaged in learning activities involving online technology
- Ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws

Role of other Subject Leaders

It is the role of the Subject Leaders to:

- Liaise with the Computing & IT Leader to develop appropriate resources to support their subject
- Ensure that IT resources are appropriately budgeted for
- Work with class teachers to ensure students use IT resources and equipment effectively in their subject
- Develop their own capability to support teaching and learning
- Embed Online Safety issues in all aspects of the curriculum and other school activities
- Supervise and guide pupils carefully when engaged in learning activities involving online technology
- Ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws

Role of the Senior Leadership Team (including Headteacher)

It is the role of the Senior Leadership Team to:

- Ensure that there is an up-to-date Computing & IT policy
- Take overall responsibility for Online Safety provision
- Be responsible for ensuring that staff receive suitable training to carry out their Online Safety roles
- Receive regular monitoring reports from the Computing & IT Leader
- Support the whole-school strategic improvement of Computing

- Ensure the Computing curriculum is adequately resourced by regular funding
- Promote the use IT to support 'Outstanding' teaching and learning across the curriculum
- Provide opportunities for the Computing & IT Leader to monitor plans, assessment and lessons
- Ensure the school uses an approved, filtered Internet Service, which complies with current statutory requirements
- To be aware of procedures to be followed in the event of a serious Online Safety incident
- Ensure that there is a system in place to monitor and support staff who carry out internal Online Safety procedures (e.g. network manager)

Role of the Governors Body (or a nominated Governor)
It is the role of the Governing Body to:

- Support with strategic implementation improvement of Computing & IT
- Monitor standards ensuring improved standards of learning and achievement in Computing
- Annually audit spending on Computing & IT
- Keep up-to-date with changes in legislation and national policy
- Ensure that the school follows all current Online Safety advice to keep the pupils and staff safe
- Review the effectiveness of the Computing & IT policy
- Support the school in encouraging parents and the wider community to become engaged in Online Safety activities