Bell Lane Primary School
Computing Policy

	Name	Signature	Date
Committee with oversight of the policy	Curriculum and Standards Committee		
Lead Person	Anisha Madhewoo	Anisha Madhewoo	May 2020
Prepared by	Anisha Madhewoo	Anisha Madhewoo	May 2020
Checked by	Harsha Patel	Harsha Patel	May 2020
Approved by Chair of Governors	Tracy Simmons	Tracy Simmons	May 2020
Document Title	Computing Policy		
Version:	**1**	**Date for next review:**	

Policy Contents

Bell Lane School believes that every child should have the right to a curriculum that champions excellence; supporting pupils in achieving to the very best of their abilities. We understand the immense value technology plays not only in supporting the Computing and whole school curriculum but overall in the day-to-day life of our school. We believe that technology can provide: enhanced collaborative learning opportunities; better engagement of pupils; easier access to rich content; support conceptual understanding of new concepts and can support the needs of all our pupils.

Our aims

- Provide an exciting, rich, relevant and challenging Computing curriculum for all pupils.
- Enthuse and equip children with the capability to use technology throughout their lives.
- Give children access to a variety of high-quality hardware, software and unplugged resources.
- Teach pupils to become responsible, respectful and competent users of data, information and communication technology.
- Teach pupils to understand the importance of governance and legislation regarding how information is used, stored, created, retrieved, shared and manipulated.
- Equip pupils with skills, strategies and knowledge that will enable them to apply to the online world, whilst minimising risks to themselves or others.
- Use technology imaginatively and creatively to inspire and engage all pupils, as well as using it to be more efficient in the tasks associated with running an effective school.
- Provide technology solutions for forging better home and school links.
- Utilise computational thinking beyond the Computing curriculum.
- Exceed the minimum government recommended/statutory guidance for programmes of study for Computing and other related legislative guidance (online safety).

Policy Expectations and Standards Brief

Technical and Infrastructure approaches

This school:

- Has the educational filtered secure broadband connectivity through the LGfL and so connects to the 'private' National Education Network;
- Uses the LGfL filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature, etc. All changes to the filtering policy is logged and only available to staff with the approved 'web filtering management' status;
- Uses USO user-level filtering where relevant, thereby closing down or opening up options appropriate to the age / stage of the students;
- Ensures network healthy through use of Sophos anti-virus software (from LGfL) etc. and network set-up so staff and pupils cannot download executable files;
- Uses individual, audited log-ins for all users - the London USO system;
- 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 or approved Learning Platform;
- Only unblocks other external social networking sites for specific purposes / Internet Literacy lessons;
- Only uses the LGfL / NEN service for video conferencing activity;
- Only uses approved or checked webcam sites;
- Has blocked pupil access to music download or shopping sites – except those approved for educational purposes at a regional or national level, such as Audio Network;
- Uses security time-outs on Internet access where practicable / useful;
- Provides *highly restricted (Safe mail) / simulated environments for e-mail with Key Stage 1 pupils*; Uses London mail with students as this has email content control and the address does not identify the student or school;
- Provides staff with an email account for their professional use, *London Staff mail / LA email* and makes clear personal email should be through a separate account;
- *Uses teacher 'remote' management control tools for controlling workstations / viewing users / setting-up applications and Internet web sites, where useful;*
- *Has additional local network auditing software installed;*
- Works in partnership with the LGfL to ensure any concerns about the system are communicated so that systems remain robust and protect students;
- 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;

Curriculum

As a school, we have chosen the Purple Mash Computing Scheme of Work from Reception to Year 6. The scheme of work supports our teachers in delivering fun and engaging lessons which help to raise standards and allow all pupils to achieve to their full potential. We are confident that the scheme of work more than adequately meets the national vision for Computing. It provides immense flexibility, strong cross-curricular links and integrates perfectly with the 2Simple Computing Assessment Tool. Furthermore, it gives excellent supporting material for less confident teachers.

Early Years

We aim to provide our pupils with a broad, play-based experience of Computing in a range of contexts. We believe the following:

- Early Years learning environments should feature ICT scenarios based on experience in the real world, such as in roleplay.
- Pupils gain confidence, control and language skills through opportunities to 'paint' on the interactive board/devices or control remotely operated toys.
- Outdoor exploration is an important aspect, supported by ICT toys such as metal detectors, controllable traffic lights and walkie-talkie sets.
- Recording devices can support children to develop their communication skills. This is especially useful for children who have English as an additional language.

Key Stage 1 outcomes

- Understand what algorithms are, how they are implemented as programs on digital devices, and that programs execute by following a sequence of instructions.
- Write and test simple programs.
- Organise, store, manipulate and retrieve data in a range of digital formats.
- Communicate safely and respectfully online, keeping personal information private, and recognise common uses of information technology beyond school.

Key Stage 2 outcomes

- 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.

Assessment

- Pupil attainment is assessed using the 2Simple Computing Assessment Tool for Years 1 to 6. The tool enables staff to accurately identify attainment of pupils through the detailed exemplification it has for each key learning intention.
- Teachers keep accurate records of pupil attainment by entering data using the Target Tracker tool.
- Tracking of attainment by using the 2Simple Computing Assessment Tool is used to inform future planning.
- Children are encouraged to self, peer and group assess work in a positive way using online collaborative tools such as 2Blog in Purple Mash.
- Formative assessment is undertaken each session/interaction in Computing and pupils are very much encouraged to be involved in that process. Through using the progression of skills documents and displays from 2Simple, both teachers and pupils can evaluate progress. Features such as preview and correct in Purple Mash are used to further support feedback and assessment.
- Summative assessment is undertaken in line with the assessment cycle (See Assessment Policy). Using electronic work samples from children's portfolios on Purple Mash, teachers enter judgements about the
- Work from a range of classes and abilities is shared using the Noticeboard feature in Purple Mash.
- Staff in Early Years use 'Evidence Me' and as a way of assessing and carrying out observations of children to keep track of their learning. It shows the impact of children's learning by capturing learners' experiences, monitoring their development, and creating reports to share their progress. Staff can easily capture observations through a variety of media on the go.

Resources

- All resources are procured with the underlining considerations of value: The extent at which the resource impacts on learning and the material cost of this. Protocol details for procurement can be found in the school finance policy.
- A range of resources is available which successfully supports delivering the Computing curriculum and enables all learners to reach their full potential.
- Resources are suitably maintained and replenished when needed, which is overseen by the Computing Leader.
- An itemised list of all resources is shared with staff and kept up to date by the Computing Leader.
- Audits of school resources are conducted regularly by the Computing Leader, which informs bidding for budgets allocations.
- The Computing Leader keeps up to date with the latest technology resources and will make informed decisions about possible procurement of them through their own research.
- Suggestions for getting the very best out of the resources are made available to teaching and support staff by the Computing Leader.
- The Computing Action Plan details foreseen future resource procurement which is shared with senior leaders before the budget setting period.

Inclusion

At Bell Lane Primary School, we aim to enable all children to achieve to their full potential. This includes children of all abilities, social and cultural backgrounds, those with disabilities, EAL speakers and SEN statement and non-statemented.

We place particular emphasis on the flexibility technology brings to allowing pupils to access learning opportunities, particularly pupils with SEN and disabilities. With this in mind, we will ensure additional access to technology is provided throughout the school day and in some cases beyond the school day.

Monitoring, Evaluation and Feedback

Monitoring standards of teaching and learning within Computing is the primary responsibility of the Computing Leader. All teachers are expected to keep an online portfolio or track children's work using Purple Mash. This portfolio must contain work samples from all areas of the curriculum taught for the year group.
Details of monitoring and evaluation schedules can be found in the Computing Action Plan and School Monitoring Schedule.
Monitoring will be achieved through:

- Work scrutiny
- Learning walks
- Observations
- Pupil voice
- Teacher voice
- Reflective teacher feedback
- Learning environment monitoring
- Dedicated Computing Leader and Assessment Leader time

Evaluation and Feedback will be achieved through:

- Dedicated Computing Leader and Assessment Leader time.
- Using recognised standards documentation for end-of-year expectations.
- Using recognised national standards for benchmarking Computing provision in primary schools.
- Written feedback on evaluation of monitoring activities to be provided by the Computing Leader in a timely manner.
- Feedback on whole school areas of development in regard to Computing to be fed back through insets/AOB/staff meetings.

Roles and Responsibilities

Due to technology extending beyond the National Curriculum for Computing, there are key roles and responsibilities specific members of staff have.

Head Teacher

- Monitoring the implementation of the Computing Policy and its associated policies such as the Safeguarding and SEND Policies.
- Ratifying (in conjunction with the Governing Body) the Computing policy, Safeguarding policy and Computing Leader's Action Plan.
- Securing technical support service contracts and infrastructure maintenance contracts.
- Approving CPD and training which is in line with the whole school's strategic plan.
- Approving budget bids and setting them.
- Creating in conjunction with the Computing Leader, a long-term vision for Computing which includes forecasted expenditure and resources.
- Monitoring the performance of the Computing Leader in respect to their specific job role description for Computing.
- Ensuring any government legislation is being met.

Computing Leader

- Raising the profile of Computing for all stakeholders.
- Monitoring the standards of Computing and feeding back to staff in a timely fashion so they can act on areas for development.
- Ensuring assessment systems are in place for Computing.
- Maintaining overall consistency in standards of Computing across the school.
- Reporting on Computing at specific times of the year to the Governing Body/Head/Staff.
- Auditing the needs of the staff in terms of training/CPD.
- Actively supporting staff with their day-to-day practice.
- Seeking out opportunities to inspire staff in developing their practice through modelling and sharing new ideas, approaches and initiatives.
- Attending training and keeping abreast with the latest educational technology initiatives.
- Using nationally recognised standards to benchmark Computing.
- Creating Action Plans for Computing and supporting a long-term vision which feeds into the whole school development plan.
- Creating bids for the annual budgets and monitoring budget spend.

- Keeping an up-to-date log of all resources available to staff.
- Procuring physical and online resources that demonstrate best value.
- Reviewing the Computing curriculum and developing it as needed.
- Overseeing the effectiveness of the technician.
- Working as needed with the SENCO/Head Teacher to ensure online safety provision is above adequate and all legislation is in place.

Technician

- Routinely checks school filtering, monitoring and virus protection.
- Sets up new hardware and installations.
- Maintains network connectivity and stability.
- Supports the Computing Leader and Head Teacher with future infrastructure needs and associated projected costs.
- Fixes errors/issues with hardware and software set-up, prioritising as needed.
- Supports the administration and set-up of online services including the school website.
- Conducts routine scheduled maintenance/updates on systems.

Administration Staff

- Maintains the school website content.
- Posts approved requests to the school's social media accounts.
- Supports procurement of resources and technical services.
- Supports the technician with some data management.

Online Safety

Safeguarding

Online safety has a high profile at Bell Lane School for all stakeholders. We ensure this profile is maintained and that pupil needs are met by the following:

- A relevant up-to-date online safety curriculum which is progressive from Early Years to the end of Year 6.
- A curriculum that is threaded throughout other curriculums and embedded in the day-to-day lives of our pupils.
- Training for staff and governors which is relevant to their needs and ultimately positively impacts on the pupils.
- Scheduled pupil voice sessions and learning walks steer changes and inform training needs.

- Through our home/school links and communication channels, parents are kept up to date with relevant online safety matters, policies and agreements. They know who to contact at school if they have concerns.
- Pupils, staff and parents have Acceptable Use Policies which are signed and copies freely available.
- Our online safety policy (part of our safeguarding policy) clearly states how monitoring of online safety is undertaken and any incidents/infringements to it are dealt with.
- Filtering and monitoring systems for all our online access.
- Data policies which stipulate how we keep confidential information secure.

Health and Safety

Bell Lane School takes all necessary measures to ensure both staff and pupils are aware of the importance of health and safety.
Both staff and pupils are trained to handle electrical equipment correctly including how to power off and on. Pupils are reminded about the dangers of electricity and the danger signs to look out for. Adequate displays and warning signs are strategically placed around the school to reinforce health and safety.

KS1 Acceptable Use Agreement

I want to feel safe and comfortable and I understand that other children want to feel the same way.

I agree that I will:

- Always keep my passwords secret
- I will only use activities that an adult has agreed
- I will take care of all of our equipment (Chromebooks, iPads, computers etc.)
- I will ask for help from an adult if I am not sure what to do or if I think I have made a mistake
- I will tell an adult if I see something that upsets me on the screen.
- I will only send messages using kind words.
- I will show my teacher if I get an unkind message.
- I will not reply to any unkind messages.
- I will not share any personal information about myself online.
- I will not load photographs of myself onto computers.
- I know that if I break the rules I might not be allowed to use IT equipment at home or school.
- I understand these rules and will follow them.
- I know that once I post a message or an item on the internet it becomes permanent and is completely out of my control.

I understand that I am responsible for my actions and the consequences. I have read and understood the above and agree to follow this agreement.

Name:

Class:

Date:

As you unable to return these forms we will be expecting that once this has been posted on twitter and class dojo all pupils and parents/carers will adhere to this.

KS2 Acceptable Use Agreement

When I am using laptops, Chromebook, iPads or phones other technologies, I want to feel safe all the time. I understand that other children also want to feel safe all of the time.

I agree that I will:

- Always keep my passwords a secret

- I understand that my use of the internet is monitored.
- I will not try to access anything that is inappropriate for my age or illegal.
- I will tell an adult if I find any damage or faults with technology, however this may have happened.
- I will only visit sites which are appropriate to my current learning.
- I will tell a trusted adult straight away if anything makes me feel scared or uncomfortable online.
- I will only send respectful, appropriate messages.
- If I receive an inappropriate message, I will show it to a trusted adult straight away.
- I will not reply to any inappropriate message or anything which makes me feel uncomfortable.
- I will not give my mobile phone number to anyone who is not a friend I have met in person.
- I will only email people I know or those approved by a responsible adult.
- I will only use email / cloud services which have been provided by school
- I always keep my personal details private.
- I will always check with a responsible adult and my parent/carer before I show photographs of myself.
- I will never meet an online friend without taking a responsible adult that I know with me.

I know that once I post a message or an item on the internet it becomes permanent and is completely out of my control.

I understand that I am responsible for my actions and the consequences. I have read and understood the above and agree to follow this agreement.

Name:

Class:

Date:

Laptop/ iPad Loan Agreement

Bell Lane Primary School and Children Centre has limited resources and finances to fund technology for staff use. If you require a laptop and / or iPad to assist you with the delivery of the curriculum, the Headteacher / governors will discuss requests on an individual basis. Equipment together with a power supply will be loaned to you while you remain employed at this school. This loan is subject to review on a regular basis, and can be withdrawn at any time.
As a member of staff to whom a laptop and/or iPad has been loaned I have read and agree to the following terms and conditions while the laptop is in my possession:

1. The laptop and/or iPad, and any accessories provided with it, remains the property of Bell Lane Primary School and Children Centre and is strictly for staff use.
2. I understand insurance cover provides protection from the standard risks but excludes theft from a vehicle. If the laptop/iPad is stolen **from an unattended vehicle** or a house left unattended for longer than 48 hours, I will be responsible for its replacement. (Check your house insurance).
3. I agree to treat the laptop/iPad with due care and keep the laptop/iPad in good condition.
4. I agree to back up my work on a regular basis. I understand the school will not accept responsibility for the loss of work in the event of the technology malfunctioning.
5. I agree that Anti-Virus software is installed and must be updated on a weekly basis. ICT staff from the school will advise on the routines and schedule of this operation. This tends to occur automatically and is overseen by the ICT Technician.
6. The laptop must be encrypted by ICT technicians and if there is any thought that it is not – I will tell someone immediately and not take off site. I will inform the DPO – Mrs Teresa Green or the Headteacher Miss Harsha Patel.
7. I will not attempt to remove any encryption.
8. Should any faults occur, I agree to notify the school's ICT staff as soon as possible so that they may undertake any necessary repairs. Under no circumstances should I, or anyone other than ICT staff, attempt to fix suspected hardware, or any other faults.
9. I agree to attend training in line with the Curriculum, the Network, Intranet, Internet and email within the school provided by ICT staff.
10. I agree that home Internet access is permitted at the discretion of the Headteacher.
11. I agree that any telephone/broadband charges incurred by staff accessing the Internet from any site other than school premises are not chargeable to the school.
12. I agree to adhere to School and LA policies regarding the following, updated as necessary:

Acceptable Use Policy even when using my laptop/iPad at home.

- Data Protection and the GDPR Policies
- Social Media
- Computer Misuse
- Health and Safety

13. I agree to make sure that I lock my laptop/iPad away at the end of the day in order to validate the school's insurance should it be stolen. If it is lost or stolen, I will inform the DPO immediately.

Laptop/ IPAD Details

Laptop Make		Model	
iPad Make		Model	

I have read, understand and will comply by the school's laptop/ iPad loan agreement.

Staff member		Date	
Headteacher		Date	

COVID-19 addendum

This addendum has been developed as an addition to our school's Online Safety Policy, to assist in maintaining and appropriately adapting our online safeguarding roles and responsibilities during this pandemic. This policy will be amended and updated with government Covid-19 guidance as and when this is published. **Coronavirus (COVID-19): guidance for schools and other educational settings**

Coronavirus: safeguarding in schools, colleges and other providers

https://www.gov.uk/guidance/safeguarding-and-remote-education-during-coronavirus-covid-19

Please refer to the Corona virus Risk Assessment also available here on our school website http://www.belllaneprimaryschool.co.uk/

We will still have regard to the statutory safeguarding guidance, **Keeping Children Safe in Education** and relevant government coronavirus guidance such as **Coronavirus: safeguarding in schools, colleges and other providers, The Prevent Duty advice for schools and childcare providers** and **Prevent duty guidance** to ensure we keep children safe.

This addendum applies during the period of school closure due to COVID-19, reflects updated advice from our Prevent partners and is a supplement to our existing Online Safety and Child Protection Policies which are still operational.

This addendum will also reflect any updated advice from Barnet Safeguarding Children Partnership and from the Local Authority in relation to online safety and our Prevent duties.

Details of the Prevent radicalisation and community safety guidance: https://www.barnet.gov.uk/community/community-safety/radicalisation-and-prevent

Thebarnetscp.org.uk

Key Online Safety and Prevent contacts during Covid-19 arrangements

Role	Name	Contact details
Headteacher	Harsha Patel	children@belllane.barnet.sch.uk
Designated Safeguarding Lead including Prevent Lead	Harsha Patel	children@belllane.barnet.sch.uk
Data Protection Officer	Teresa Green	tgreen@belllane.barnet.sch.uk
Designated member of senior leadership team if DSL (and deputy) can't be on site	Janice Doherty	jdoherty@belllane.barnet.sch.uk
	Victoria Atkin	vatkin@belllane.barnet.sch.uk
	Anisha Madhewoo	amadhewoo@belllane.barnet.sch.uk
	Tamsin Jones	tjones@belllane.barnet.sch.uk
	Caroline Walsh	cwalsh@belllane.barnet.sch.uk
	Sharon Plummeridge	splummeridge@belllane.barnet.sch.uk
	Boadicea Faulkner	bfaulkner@belllane.barnet.sch.uk
Link Governor for online safety	Tracy Simmons	tsimmons@belllane.barnet.sch.uk
Designated Prevent Governor/Trustee:	Tracy Simmons	tsimmons@belllane.barnet.sch.uk

Note: Contact details for all other key safeguarding agencies are as referenced in our Child Protection Policy. This includes Barnet MASH, for pupils displaying concerning behaviour and Due Diligence and Counter Extremism Division of the DfE for concerns about staff.

Barnet Multiagency Safeguarding Hub: 020 8359 4066; mash@barnet.gov.uk

DfE Counter Extremism Division: DDCED.SPOE@education.gov.uk

Please use this Online Tool for Reporting Terrorist or Extremist Use of the Internet.

Reporting Harmful or upsetting content:

- reporting harmful online content to the UK Safer Internet Centre
- getting government advice and trusted resources from Educate Against Hate on safeguarding from radicalisation, building resilience to extremism, and promoting shared values

Personal data and our duty under GDPR

The school's Data Protect Policy remains in operation.

During this period of remote learning and working it is even more important that we consider how safely personal data is being shared.

- Bell Lane Primary School will ensure that access to data systems is provided, to staff who need access, securely.
- Staff will be careful when sharing personal data for access to online resources.
- Only share contact details for themselves or others when necessary to relevant staff or agencies.

Safeguarding

Many staff will be working remotely with pupils and this can be challenging. However, we must not lose sight of our overarching responsibly to safeguard pupils both in school and working online at home. Therefore, it is vital that we all follow these important safeguarding principles:

- The best interests of children must always continue to come first
- If anyone has a safeguarding concern about any child, they should continue to act on it immediately and report to the DSL
- Children should continue to be protected when they are online.
- Online advice and guidance will be shared with parents who are caring for children at home.

- Safe practice guidelines will be followed for virtual classrooms and videoconferencing.
- Ensure, wherever possible, children being educated at home are aware of the enhanced online risks encountered during the virus lockdown from conspiracy theories, fake news and extremist groups.
- Promote and monitor good online behaviours
- Ensure that pupils have access to pastoral support
- Reporting concerns to the DSL

Further advice and guidance on Prevent can be obtained from:

Prevent Education Officer: perryn.jasper@barnet.gov.uk; 07856 002586; 020 8359 7371

Prevent Coordinator: sam.rosengard@barnet.gov.uk; 07921 277713; 020 8359 3323

Bullying or abuse online

Any abusive behaviour will not be tolerated, this includes online bullying and any abusive, racist or derogatory comments made online.

Anti-bullying policy

Other sources of advice and information can be found:

- get advice on reporting online abuse from the National Crime Agency's Child Exploitation and Online Protection command
- get advice and support from Anti-Bullying Alliance for children who are being bullied
- Schools can access the free Professionals Online Safety Helpline which supports the online safeguarding of both children and professionals. Call 0344 381 4772 or email helpline@saferinternet.org.uk. The helpline is open from Monday to Friday from 10am to 4pm.

All concerns should be reported following normal procedures

Online safety in school

We will continue to have appropriate filtering and monitoring systems in place in school.

Where students are using computers in school, appropriate supervision will be in place.

Online safety when working remotely

Where staff are interacting with children online, they will continue to follow our existing staff behaviour policy/code of conduct.

It is important that all staff who interact with children, including online, continue to look out for signs a child may be at risk. Any such concerns should be dealt with as the existing Child Protection / Safeguarding Policy directs. Where appropriate referrals should still be made to children's Multiagency Safeguarding Hub and when required, the police.

Online teaching should follow the same principles as set out in the staff Code of Conduct Policy and the Behaviour Policy.

The school/college will ensure any use of online learning tools and systems is in line with privacy and data protection/GDPR requirements.

Below are some things to consider when delivering virtual lessons, especially where webcams are involved:

- Where 1 to 1 communication is required, the pupil should have an appropriate adult present.
- Staff and children must wear suitable clothing, as should anyone else in the household.
- Any computers used should be in appropriate areas, for example, not in bedrooms; and the background should be blurred where the technology is available.
- The live class should be recorded so that if any issues were to arise, the video can be reviewed.
- Live classes should be kept to a reasonable length of time.
- Language must be professional and appropriate, including any family members in the background.
- Staff must only use communication systems provided by the school/college to communicate with learners.
- Staff should record, the length, time, date and attendance of any sessions held.

If IT staff are unavailable, our contingency plan is (*insert details of contingency plans for IT support, e.g. from another school, LA etc.)*

Acceptable use of technology – refer to online safety tab on the school website,

Other sources of advice:

- remote education advice from The Key for School Leaders
- advice from NSPCC on undertaking remote education safely

- guidance from the UK Safer Internet Centre on remote education

Guidance on teaching online safety in schools provides information to help schools ensure their pupils understand how to stay safe and behave online.

Staff will continue to be alert to signs that a child may be at risk of harm online, and act on any concerns immediately, following our normal reporting and record keeping procedures.

We will make sure children know how to report any concerns they have back to our school, and signpost them to other sources of support when required.

Staff working safely

Safe practice guidelines will be followed for virtual classrooms and videoconferencing. This includes:

- Always two members of staff for online classrooms
- Never be alone with a pupil
- Wearing appropriate clothing
- Ensuring the background to your presentation is appropriate
- New material is checked by SLT or your Line Manager
- The platform e.g. Zoom, Skye, email etc. for your presentation is approved, never use a personal account
- Ensure that only school approved electronic equipment is used
- Report any breaches of data protection to the DPO (or as applicable)
- Report any unexpected events such as an unplanned call from a parent etc.
- Report any cyber bombing
- Report or document (dependent on school policy) any incident in your house that was seen by pupils.
- Report any inappropriate behaviour of other adults online e.g. a parent in the background swearing.
- Remember that you are teaching a class

Working with parents and carers

We will make sure parents and carers:

- Are aware of the potential risks to children online and the importance of staying safe online.
- Know what our school is asking children to do online, including what sites they will be using and who they will be interacting with from our school.
- Communicate within school hours as much as possible (or hours agreed with the school to suit the needs of staff)
- communicate through the school channels approved by the senior leadership team
- use school email accounts (not personal ones)
- use school devices over personal devices wherever possible

- advise teachers not to share personal information
- Are aware that they should only use reputable online companies or tutors if they wish to supplement the remote teaching and resources our school provides.
- Know where else they can go for support to keep their children safe online.

We will do this by sharing information via e-newsletters, text messages (remove if this is not available) and information posted on our website, following updates and advice received from:

Safer Internet Centre

DfE advice and guidance

London Grid for Learning

ThinkUKnow

Educateagainsthate.com/parents/

https://parentinfo.org/

https://www.childnet.com/parents-and-carers/parent-and-carer-toolkit

Education and training:

- At Bell Lane, we encourage pupils to tell a teacher / responsible adult immediately if they encounter any material that makes them feel uncomfortable;
- Teaches pupils and informs staff what to do if they find inappropriate web material i.e. to switch off monitor and report the URL to the teacher or System Manager.
- Ensures pupils and staff know what to do if there is a cyber-bullying incident;
- Ensures all pupils know how to report any abuse;
- Has a clear, progressive e-safety education programme throughout all Key Stages, built on LA / London / national guidance. Pupils are taught a range of skills and behaviours appropriate to their age and experience, such as:

    - to STOP and THINK before they CLICK
    - to discriminate between fact, fiction and opinion;
    - to develop a range of strategies to validate and verify information before accepting its accuracy;
    - to skim and scan information;
    - 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 'Netiquette' 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;

- 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 observe and respect copyright / intellectual property rights;
- Ensures that staff and pupils understand the issues around aspects of the commercial use of the Internet, as age appropriate. This may include, risks in pop-ups; buying on-line; on-line gaming / gambling;
- 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 training available annually to staff on the e-safety education program;
- Runs a rolling programme of advice, guidance and training for parents, including:
  - Information leaflets; in school newsletters; on the school web site;
  - Workshops
  - Suggestions for safe Internet use at home-these are also be posted on our class dojo and Twitter pages

Statutory Guidance and Legislation

Acts Relating to Monitoring of Staff email

Data Protection Act 1998

The Act requires anyone who handles personal information to comply with important data protection principles when treating personal data relating to any living individual. The Act grants individuals' rights of access to their personal data, compensation and prevention of processing.

http://www.hmso.gov.uk/acts/acts1998/19980029.htm

The Telecommunications (Lawful Business Practice)

(Interception of Communications) Regulations 2000

http://www.hmso.gov.uk/si/si2000/20002699.htm

Regulation of Investigatory Powers Act 2000

Regulating the interception of communications and making it an offence to intercept or monitor communications without the consent of the parties involved in the communication. The RIP was enacted to comply with the Human Rights Act 1998. The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, however, permit a degree of monitoring and record keeping, for example, to ensure communications are relevant to school activity or to investigate or detect unauthorised use of the network. Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored. Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation.

http://www.hmso.gov.uk/acts/acts2000/20000023.htm

Human Rights Act 1998

http://www.hmso.gov.uk/acts/acts1998/19980042.htm

Other Acts Relating to eSafety

Racial and Religious Hatred Act 2006

It a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Sexual Offences Act 2003

The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. Schools should already have a copy of "*Children & Families: Safer from Sexual Crime*" document as part of their child protection packs.

For more information www.teachernet.gov.uk

Communications Act 2003 (section 127)

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

The Computer Misuse Act 1990 (sections 1 – 3)

Regardless of an individual's motivation, the Act makes it a criminal offence to gain:

- access to computer files or software without permission (for example using another person's password to access files)
- unauthorised access, as above, in order to commit a further criminal act (such as fraud)
- impair the operation of a computer or program

UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences.

Malicious Communications Act 2000

This legislation makes it a criminal offence to send an electronic message (e-mail) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety.

Copyright, etc. and Trade Marks (Offences and Enforcement) Act 2002

Copyright is the right to prevent others from copying or using work without permission. Works such as text, music, sound, film and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer. Copyright infringement is to copy all or a substantial part of anyone's work without obtaining them author's permission. Usually a license associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a license before you copy or use someone else's material. It is also illegal to adapt or use software without a license or in ways prohibited by the terms of the software license.

Public Order Act 1986 (sections 17 – 29)

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

Protection of Children Act 1978 (Section 1)

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is a anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.

Obscene Publications Act 1959 and 1964

Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other.

A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Acts Relating to the Protection of Personal Data

Data Protection Act 1998
http://www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_1

The Freedom of Information Act 200
http://www.ico.gov.uk/for_organisations/freedom_of_information_guide.aspx

Managing e-Mail

- The school gives all staff their own e-mail account to use for all school business as a work-based tool This is to minimize the risk of receiving unsolicited or malicious e-mails and avoids the risk of personal profile information being revealed
- It is the responsibility of each account holder to keep the password secure.
- Under no circumstances should staff contact pupils, parents or conduct any school business using personal e-mail addresses
- Pupils may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes
- E-mails created or received as part of your School job will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000. You must therefore actively manage your e-mail account as follows:

  - Delete all e-mails of short-term value

  - Organize e-mails into folders and carry out frequent house-keeping on all folders and archives

- All pupil e-mail users are expected to adhere to the generally accepted rules of netiquette particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in e-mail communication, or arrange to meet anyone without specific permission, virus checking attachments
- Pupils must immediately tell a teacher/ trusted adult if they receive an offensive e-mail
- Staff must inform (the eSafety coordinator/ ICT coordinator) if they receive an offensive e-mail
- Pupils are introduced to e-mail as part of the ICT Scheme of Work

- However, you access your school e-mail (whether directly, through webmail when away from the office or on non-school hardware) all the school e-mail policies apply

Sending e-mails

- Use your own school e-mail account so that you are clearly identified as the originator of a message
- Keep the number and relevance of e-mail recipients, particularly those being copied, to the minimum necessary and appropriate
- Do not send or forward attachments unnecessarily. Whenever possible, send the location path to the shared drive rather than sending attachments
- School e-mail is not to be used for personal advertising

Receiving e-Mails

- Check your e-mail regularly
- Activate your 'out-of-office' notification when away for extended periods
- Never open attachments from an untrusted source; Consult your network manager first.
- Do not use the e-mail systems to store attachments. Detach and save business related work to the appropriate shared drive/folder
- The automatic forwarding and deletion of e-mails is not allowed

E-mailing Personal, Sensitive, Confidential or Classified Information

- Assess whether the information can be transmitted by other secure means before using e-mail, e-mailing confidential data is not recommended and should be avoided where possible
- The use of Hotmail or any other Internet based webmail service for sending e-mail containing sensitive information is not permitted

    - Do not send information to anybody/person whose details you have been unable to separately verify (usually by phone)
    - Send the information as an encrypted document **attached** to an e-mail
    - Provide the encryption key or password by a **separate** contact with the recipient(s)
    - Do not identify such information in the subject line of any e-mail
    - Request confirmation of safe receipt

ESafety & Incident Reporting

ESafety - Roles and Responsibilities

As eSafety is an important aspect of strategic leadership within the school, the Head and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named eSafety coordinator in this school is the IT leader who has been designated this role as a member of the senior leadership team. All members of the school community have been made aware of who holds this post.

Senior Management and Governors are updated by the Head/ eSafety coordinator and all governors have an understanding of the issues and strategies at our school in relation to local and national guidelines and advice.

This policy, supported by the school's acceptable use agreements for staff, governors, visitors and pupils, is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: child protection, health and safety, home–school agreements, and behavior/pupil discipline (including the anti-bullying) policy and PSHE

e-Safety in the Curriculum

ICT and online resources are increasingly used across the curriculum. We believe it is essential for eSafety guidance to be given to the pupils on a regular and meaningful basis. eSafety is embedded within our curriculum and we continually look for new opportunities to promote eSafety. The school provides opportunities within a range of curriculum areas to teach about eSafety. Pupils are educated on the dangers of technologies that maybe encountered outside school is done informally when opportunities arise and as part of the eSafety curriculum

e-Safety Skills Development for Staff

- New staff receive information on the school's acceptable use policy as part of their induction
- All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of eSafety and know what to do in the event of misuse of technology by any member of the school community (see enclosed flowchart)
- All staff are encouraged to incorporate eSafety activities and awareness within their curriculum areas

Managing the School eSafety Messages

- We endeavour to embed eSafety messages across the curriculum whenever the internet and/or related technologies are used
- The eSafety policy will be introduced to the pupils at the start of each school year

- eSafety posters will be prominently displayed

Managing Other Web 2 Technologies

Web 2, including social networking sites, if used responsibly both outside and within an educational context can provide easy to use, creative, collaborative and free facilities. However, it is important to recognise that there are issues regarding the appropriateness of some content, contact, culture and commercialism. To this end, we encourage our pupils to think carefully about the way that information can be added and removed by all users, including themselves, from these sites.

- At present, the school endeavours to deny access to social networking sites to pupils within school

- All pupils are advised to be cautious about the information given by others on sites, for example users not being who they say they are

- Pupils are taught to avoid placing images of themselves (or details within images that could give background details) on such sites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online

- Pupils are always reminded to avoid giving out personal details on such sites which may identify them or where they are (full name, address, mobile/ home phone numbers, school details, IM/ email address, specific hobbies/ interests)

- Our pupils are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals

- Pupils are encouraged to be wary about publishing specific and detailed private thoughts online

- Our pupils are asked to report any incidents of bullying to the school

- Staff may only create blogs, wikis or other web 2 spaces in order to communicate with pupils using the LA Learning Platform or other systems approved by the Headteacher

Parental Involvement

We believe that it is essential for parents/ carers to be fully involved with promoting eSafety both in and outside of school and also to be aware of their responsibilities. We regularly consult and discuss eSafety with parents/ carers and seek to promote a wide understanding of the benefits related to ICT and associated risks.

- Parents/carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to school

- Parents/carers are required to make a decision as to whether they consent to

images of their child being taken/ used in the public domain (e.g., on school website)

We will support the school approach to on-line safety and not deliberately upload or add any images, sounds or text that could upset or offend any member of the school community

- The school disseminates information to parents relating to eSafety where appropriate in the form of;

    - Information and celebration evenings
    - Posters
    - Website/ Learning Platform postings
    - Newsletter items
    - Learning platform training

Passwords and Password Security

Passwords

- Always use your own personal passwords to access computer-based services
- Make sure you enter your personal passwords each time you logon. Do not include passwords in any automated logon procedures
- Staff should change temporary passwords at first logon
- Change passwords whenever there is any indication of possible system or password compromise
- Do not record passwords or encryption keys on paper or in an unprotected file
- Only disclose your personal password to authorised ICT support staff when necessary, and never to anyone else. Ensure that all personal passwords that have been disclosed are changed once the requirement is finished
- Passwords must contain a minimum of six characters and be difficult to guess
- User ID and passwords for staff and pupils who have left the School are removed from the system within 1 day

Password Security

Password security is essential for staff, particularly as they are able to access and use pupil data. Staff are expected to have secure passwords which are not shared with anyone. The pupils are expected to keep their passwords secret and not to share with others, particularly their friends. Staff and pupils are regularly reminded of the need for password security.

- Users are provided with a Learning Platform and Management Information System (where appropriate) log-in username.
- Pupils are not allowed to deliberately access on-line materials or files on the school network, of their peers, teachers or others
- Staff are aware of their individual responsibilities to protect the security and confidentiality of school networks, MIS systems and/or Learning Platform, including ensuring that passwords are not shared and are changed periodically. Individual

staff users must also make sure that workstations are not left unattended and are locked.

- Due consideration should be given when logging into the Learning Platform to the browser/cache options (shared or private computer)

Protecting Personal, Sensitive, Confidential and Classified Information

- Ensure that any School information accessed from your own PC or removable media equipment is kept secure
- Ensure you lock your screen before moving away from your computer during your normal working day to prevent unauthorised access
- Ensure the accuracy of any personal, sensitive, confidential and classified information you disclose or share with others
- Ensure that personal, sensitive, confidential or classified information is not disclosed to any unauthorised person
- Ensure the security of any personal, sensitive, confidential and classified information contained in documents you fax, copy, scan or print. This is particularly important when shared copiers (multi-function print, fax, scan and copiers) are used and when access is from a non-school environment
- Only download personal data from systems if expressly authorised to do so by your manager
- You must not post on the internet personal, sensitive, confidential, or classified information, or disseminate such information in any way that may compromise its intended restricted audience.
- Keep your screen display out of direct view of any third parties when you are accessing personal, sensitive, confidential or classified information
- Ensure hard copies of data are securely stored and disposed of after use in accordance with the document labeling
- Ensure the security of any personal, sensitive, confidential and classified information contained in documents you fax, copy, scan or print. This is particularly important when shared copiers (multi-function print, fax, scan and copiers) are used and when access is from a non-school environment
- Only download personal data from systems if expressly authorised to do so by your manager
- You must not post on the internet personal, sensitive, confidential, or classified information, or disseminate such information in any way that may compromise its intended restricted audience.
- Keep your screen display out of direct view of any third parties when you are accessing personal, sensitive, confidential or classified information
- Ensure hard copies of data are securely stored and disposed of after use in accordance with the document labelling

Remote Access

- You are responsible for all activity via your remote access facility
- Only use equipment with an appropriate level of security for remote access
- To prevent unauthorised access to School systems, keep all dial-up access information such as telephone numbers, logon IDs and PINs confidential and do not disclose them to anyone
- Select PINs to ensure that they are not easily guessed, e.g. do not use your house or telephone number or choose consecutive or repeated numbers
- Avoid writing down or otherwise recording any network access information. Any such information that is written down must be kept in a secure place and disguised so that no other person will be able to identify what it is
- Protect School information and data at all times, including any printed material produced while using the remote access facility. Take particular care when access is from a non-School environment

Images and Photography

Use of Images

Digital images are easy to capture, reproduce and publish and, therefore, misuse. We must remember that it is not always appropriate to take or store images of any member of the school community or public, without first seeking consent and considering the appropriateness.

- With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment
- Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, this includes when on field trips.
- Pupils are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of the others, this includes when on field trips

Consent of Adults Who Work at the School

Permission to use images of all staff who work at the school is sought on induction and a copy is located in the personnel file

Storage of Images

- Images/ films of children are stored on the school's network
- Pupils and staff are not permitted to use personal portable media for storage of images (e.g., USB sticks) unless they are password encrypted USB sticks.
- Rights of access to this material are restricted to the teaching staff and pupils

within the confines of the school network/ Learning Platform

- The Senior Leadership Team has the responsibility of directing the deletion of the images when they are no longer required, or the pupil has left the school

Hardware, Removable Media and Mobile Technologies

School IT Equipment

- As a user of IT, you are responsible for any activity undertaken on the school's IT equipment provided to you

- It is recommended that schools log IT equipment issued to staff and record serial numbers as part of the school's inventory

- Do not allow your visitors to plug their IT hardware into the school network points (unless special provision has been made). They should be directed to the wireless IT Facilities if available

- Ensure that all IT equipment that you use is kept physically secure

- Do not attempt unauthorised access or make unauthorised modifications to computer equipment, programs, files or data. This is an offence under the Computer Misuse Act 1990

- It is imperative that you save your data on a frequent basis to the school's network drive. You are responsible for the backup and restoration of any of your data that is not held on the school's network drive

- Personal or sensitive data should not be stored on the local drives of desktop PCs and laptops. If it is necessary to do so the local drive must be encrypted

- It is recommended that a time locking screensaver is applied to all machines. Any laptops etc. accessing personal data must have a locking screensaver as must any user profiles

- Privately owned IT equipment should not be used on a school network

- On termination of employment, resignation or transfer, return all IT equipment to your Manager. You must also provide details of all your system logons so that they can be disabled

- It is your responsibility to ensure that any information accessed from your own PC or removable media equipment is kept secure, and that no personal, sensitive, confidential or classified information is disclosed to any unauthorised person

- All IT equipment allocated to staff must be authorised by the appropriate Line Manager. Authorising Managers are responsible for:

    - maintaining control of the allocation and transfer within their Unit
    - recovering and returning equipment when no longer needed

All redundant IT equipment is disposed of in accordance with Waste Electrical and Electronic Equipment (WEEE) directive and Data Protection Act (DPA)

Mobile Technologies

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalized learning and 1:1 device ownership for children and young people. Many existing mobile technologies such as portable media players, PDAs, gaming devices, mobile and Smart phones are familiar to children outside of school too. They often provide a collaborative, well-known device with possible internet access and thus open up risk and misuse associated with communication and internet use. Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed. Our school chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

Personal Mobile Devices (including phones)

- The school allows staff to bring in personal mobile phones and devices for their own use. Under no circumstances does the school allow a member of staff to contact a pupil or parent/ carer using their personal device
- Pupils are not allowed to bring personal mobile devices/phones to school This technology may be used. Year 6 pupils may request permission from the Headteacher to bring a mobile phone into school but it must be kept safe in the school office and picked up at 3.30pm.
- The school is not responsible for the loss, damage or theft of any personal mobile device.
- The sending of inappropriate text messages between any member of the school community is not allowed
- Permission must be sought before any image or sound recordings are made on these devices of any member of the school community
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device

School Provided Mobile Devices (including phones)

- The sending of inappropriate text messages between any member of the school community is not allowed
- Permission must be sought before any image or sound recordings are made on the devices of any member of the school community
- Where the school provides mobile technologies such as phones, laptops and PDAs for offsite visits and trips, only these devices should be used
- Where the school provides a laptop for staff, only this device may be used to conduct school business outside of school

Telephone Services

You may make or receive personal telephone calls provided:

1. They are infrequent, kept as brief as possible and do not cause

annoyance to others

2. They are not for profit or to premium rate services

3. They conform to this and other relevant HCC and school policies.

- School telephones are provided specifically for school business purposes and personal usage is a privilege that will be withdrawn if abused

- Be aware that the laws of slander apply to telephone calls. Whilst a telephone call may seem to have a temporary and private existence it still qualifies as admissible evidence in slander law cases

- Ensure that your incoming telephone calls can be handled at all times

- Follow the appropriate procedures in the event of receiving a telephone call containing a bomb threat. These procedures should be made readily available throughout your office. If you do not have a copy, please ask your unit manager

Guidance for Emerging Technologies

Internet policy and procedures: background information

Owing to the international scale and linked nature of information available via the Internet, it is not possible to guarantee that unsuitable material will never appear. **Supervision is the key strategy.** Whatever systems are in place, something could go wrong which places pupils in an embarrassing or potentially dangerous situation.

Surfing the Web

Aimless surfing should never be allowed. It is good practice to teach pupils to use the Internet in response to an articulated need – e.g. a question arising from work in class. Children should be able to answer the question "Why are we using the Internet?"

Search engines can be difficult to use effectively and pupils can experience overload and failure if the set topic is too open-ended. It is not sensible to have younger pupils 'searching the Internet'.

Pupils do not need a thousand Web sites on weather. A small selection will be quite enough choice, and as with other resources, the teacher needs to have checked and selected them so they are appropriate for the age group and fit for purpose. Favourites/bookmarks are a useful way to present this choice to pupils.

Teachers' web site selections for various topics can be put onto a topic page on the Learning Platform so pupils can, access out of school, from home etc. Some schools put links on their school web site, although there may even be difficulties here. Hackers can infiltrate a site or take over the domain, resulting in a previously acceptable site suddenly changing. Therefore, sites should always be previewed and checked, and work for children is best located on the closed Learning Platform.

Search Engines

Some common Internet search options are high risk, for example 'Google' image search. Some LAs and Councils block this. Others keep it unblocked because it can be a useful

tool for teachers looking for images to incorporate in teaching. Where used – it must be with extreme caution. Google image search can be set-up to run in 'safe' mode although this is not fully without risk. Talk to your network manager or Technical support provider about this. LGfL guidance is available on the safety site.

Images usually have copyright attached to them which is an issue commonly overlooked but a key teaching point to pupils and staff.

Collaborative Technologies

There are a number of Internet technologies that make interactive collaborative environments available. Often the term 'Social networking software' is used. Examples include blogs (personal web-based diary or journals), wikis (modifiable collaborative web pages), and podcast sites (subscription-based broadcast over the web) supported by technologies such as RSS (really simple syndication – an XML format designed for sharing news across the web). Using these technologies for activities can be motivational, develop oracy and presentations skills, helping children consider their content and audience. Schools are best protected by using the social collaboration tools within the school's Learning Platform, such as the London MLE..

Webcams and Video Conferencing

Webcams: are used to provide a 'window onto the world' to 'see' what it is like somewhere else. LGfL has a number of nature cams showing life inside bird boxes for example and a plethora of weather cams across London providing detailed real-time weather data. Webcams can also be used across London for streaming video as part of a video conferencing project.

Video conferencing provides a 'real audience' for presentations and access to places and professionals – bringing them into the classroom. For large group work high quality video conferencing hardware equipment is required to be plugged into the network. LGfL, and the other national regional grids for learning, have made an agreement with JVCS (the Janet Videoconferencing Service) to host calls. All conferences are therefore timed, closed and safe. This is a service that is included in LGfL 2.

Pupils can search on the Internet for other webcams - useful in subject study such as geography (e.g. to observe the weather or the landscape in other places). However, there are risks as some webcam sites may contain, or have links to adult material. In schools' adult sites would normally be blocked but teachers need to preview any webcam site to make sure it is what they expect before ever using with pupils.

The highest risks lie with streaming webcams [one-to-one chat / video] that pupils use or access outside of the school environment. Pupils need to be aware of the dangers.

Social Networking Sites

These are a popular aspect of the web for young people. Sites such as Instagram, Facebook, TikTok, Snapchat, YouTube, Twitter, allow users to share and post web sites, videos, podcasts etc. It is important for children to understand that these sites are public spaces for both children and adults. They are environments that should be used with

caution. Users, both pupils and staff, need to know how to keep their personal information private and set-up and use these environments safely.

Most schools will block such sites. However, pupils need to be taught safe behaviour as they may well be able to readily access them outside of school. There are educational, monitored services that schools can purchase. Additionally, the LGfL Learning Platform provides a safe environment for pupils to share resources, store files in an ePortfolio, and communicate with others through 'closed' discussions, etc.

Podcasts

Podcasts are essentially audio files published online, often in the form of a radio show but can also contain video. Users can subscribe to have regular podcasts sent to them and simple software now enables children to create their own radio broadcast and post this onto the web. Children should be aware of the potentially inappropriate scope of audience that a publicly available podcast has and to post to safer, restricted educational environments such as the LGfL. Podcast central area.

http://www.lgfl.net/SERVICES/CURRICULUM/Pages/Podcasting.aspx

Chatrooms

Many sites allow for 'real-time' online chat. Pupils should be taught to understand the importance of safety within any chat room because they are most likely at risk out of school where they may access chatrooms such as Kik messenger, calculator apps, omegle, YOLO, House party, Whisper.

Sanctions and infringements

The school's Internet e-safety / Acceptable Use policy needs to be made available and explained to staff / Governors, pupils and parents, with all signing acceptance / agreement forms appropriate to their age and role. The school needs to have made clear possible sanctions for infringements.

Following any incident that indicates that evidence of indecent images or offences concerning child protection may be contained on school computers, the matter should be immediately referred to the Police. There are many instances where schools, with the best of intentions, have commenced their own investigation prior to involving the police. This has resulted in the loss of valuable evidence both on and off the premises where suspects have inadvertently become aware of raised suspicions. In some circumstances this interference may also constitute a criminal offence.