EXCELLENCE · VIRTUE · DEVOTION

AVANTI COURT

PRIMARY SCHOOL

Online Safety Policy

The Acceptable Use of the Internet and related Technologies

Agreed & Ratified:	Review date:
October 2022	October 2023

Contents

Overview

Online safety is an integral part of safeguarding and requires a whole school, cross-curricular approach and collaboration between key school leads. Accordingly, this policy is written in line with ‘Keeping Children Safe in Education’ 2021 (KCSIE), ‘Teaching Online Safety in Schools’ 2019, statutory RSHE guidance and other statutory documents. It complements existing and forthcoming subjects including Health, Relationships and Sex Education, Citizenship and Computing; it is designed to sit alongside your school’s statutory Safeguarding Policy. Any issues and concerns with online safety must follow the school’s safeguarding and child protection procedures.

Internet

Whilst ICT is exciting and beneficial in and out of education, web based resources are not well policed. All users are aware of the range of risks associated with the use of these internet technologies and their individual responsibilities relating to the safeguarding of children and themselves, in school and at home. Educating pupils on the dangers of technologies that maybe encountered outside school is done through the icompute curriculum and informally such as assemblies and reminders to pupils when using technology and devices connected to the Internet. Pupils are aware of the impact of Cyber bullying and know how to seek help if they are affected by any form of online bullying. All staff should be aware that safeguarding issues could manifest via peer on peer abuse. This is most likely to include, but may not be limited to, bullying (including cyber bullying), gender based violence/sexual assaults and sexting. Staff should be clear as to the school or college’s policy and procedures with regards to peer on peer abuse and how to report any concerns to the Designated Safeguarding Lead.

Managing the Internet

The school maintains that pupils will have supervised access to Internet resources through the school’s fixed and mobile internet technology. All staff will preview any recommended sites before use.
Raw image searches are discouraged when working with pupils. If internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work. Parents will be advised to supervise any further research.
Pupils at Avanti Court are too young to use social networking sites, such as Facebook (the legal age limit is 13 years old). However, we recognise the possibility of children accessing the sites at home and we provide information annually or as necessary to ensure privacy levels are high and children are aware of the risks.

Online safety risks are traditionally categorised as one of the 3 Cs: Content, Contact or Conduct (identified by Professor Tanya Byron’s 2008 report “Safer children in a digital world”). These three areas remain a helpful way to understand the risks and potential school response, whether technological or educational. They do not stand in isolation, however, and it is important to understand the interplay between all three.

Many of these new risks are mentioned in KCSIE 2021, e.g. extra-familial harms where children are at risk of abuse or exploitation to multiple harms in situations outside their families including sexual exploitation, criminal exploitation, cyber crime, serious youth violence, upskirting and sticky design.

School Policy in brief

At Avanti Court we have an Acceptable Use policy, which is reviewed at least annually, which all staff, SSC members (School Stakeholder Committee members) and visitors sign. Copies are kept on file. We use the Local Authority model policy.
All servers are managed by our designated technicians.

We use and follow LGFL back-up procedures for the office server.

We use Avanti Trust IT Engineers for disaster recovery on our admin server.

Disposal: Protected and restricted material electronic files must be securely overwritten and other media must be shredded, incinerated or otherwise disintegrated for data. At Avanti Court we use the Authority's recommended current disposal firm for disposal of system hard drives where any protected or restricted data has been held. Paper based sensitive information is stored in confidential waste bins and disposed of by a registered company. Laptops used by staff at home where used for any protected data are brought in and disposed of through the same procedure.

Security policies are reviewed by our Computing Lead and updated at least annually. Staff are aware of whom to report any incidents to, where data protection may have been compromised.

Our online safety Policy has been written by the school, building on the London Grid for Learning (LGfL) exemplar policy and Becta guidance and the Keeping Children Safe document 2021. It is reviewed annually.

Context

Harnessing Technology: Transforming learning and children's services1 sets out the government plans for taking a strategic approach to the future development of ICT.
"The Internet and related technologies are powerful tools, which open up new prospects for communication and collaboration. Education is embracing these new technologies as they bring with them fresh opportunities for both teachers and learners.
To use these technologies effectively requires an awareness of the benefits and risks, the development of new skills, and an understanding of their appropriate and effective use both in and outside of the classroom." DfES, eStrategy 2005
The Green Paper Every Child Matters2 and the provisions of the Children Act 20043, Working Together to Safeguard Children4 sets out how organisations and individuals should work together to safeguard and promote the welfare of children.

The 'staying safe' outcome includes aims that children and young people are: Safe from maltreatment, neglect, violence and sexual exploitation Safe from accidental injury and death Safe from bullying and discrimination safe from crime and anti-social behaviour in and out of school Secure, stable and cared for.

Much of these aims apply equally to the 'virtual world' that children and young people will encounter whenever they use ICT in its various forms. For example, we know that the internet has been used for grooming children and young people with the ultimate aim of exploiting them sexually; we know that ICT can offer new weapons for bullies, who may torment their victims via websites or text messages; and we know that children and young people have been exposed to inappropriate content when online, which can sometimes lead to their involvement in crime and anti- social behaviour.

It is the duty of the school to ensure that every child in their care is safe, and the same principles should apply to the 'virtual' or digital world as would be applied to the school's physical buildings.
This Policy document is drawn up to protect all parties– the students, the staff and the school and aims to provide clear advice and guidance on how to minimise risks and how to deal with any infringements.

1. **The Technologies**

ICT in the 21st Century has an all-encompassing role within the lives of children and adults. New technologies are enhancing communication and the sharing of information. Current and emerging technologies used in school and, more importantly in many cases, used outside of school by children include:

- The Internet
- e-mail
- Instant messaging -often using simple web cams
- Blogs (an on-line interactive diary)
- Podcasting (radio / audio broadcasts downloaded to computer or MP3/4 player)
- Social networking sites
- Video broadcasting sites (Popular: http://www.youtube.com/)
- Chat Rooms
- Gaming Sites
- Music download sites
- Mobile phones with camera and video functionality
- Phones with e-mail, web functionality and cut down 'Office' applications.

2. **Whole school approach to the safe use of ICT**

Creating a safe ICT learning environment includes three main elements at this school:

- An effective range of technological tools
- Policies and procedures
- Clear roles and responsibilities

A comprehensive e-Safety education programme for pupils, staff and parents.
Reference: Becta- E-safety Developing whole school policies to support effective practice 5

Roles and Responsibilities

This school is a community and all members have a duty to behave respectfully online and offline, to use technology for teaching and learning and to prepare for life after school, and to immediately report any concerns or inappropriate behaviour, to protect staff, pupils, families and the reputation of the school. We learn together, make honest mistakes together and support each other in a world that is online and offline at the same time.

Online safety is recognised as an essential aspect of strategic leadership in this school and the Head, with the suppo~~rt of the SSC, aims to embed s~~afe practices into the culture of the school. The Headteacher ensures that the Policy is implemented and compliance with the Policy monitored.

Our school Online Safety Co-ordinator is: Miss Q Khan

Our online safety Coordinator ensures they keep up to date with online issues and guidance through liaison with the Local Authority online safety Officer and through organisations such as Becta and The Child Exploitation and Online Protection (CEOP)6. The school's e-Safety coordinator ensures the Head, Senior Leadership Team and SSC members are updated as necessary.

School Stakeholder Committee members need to have an overview understanding of online safety issues and strategies at this school. We ensure our SSC members are aware of our local and national guidance on e-Safety and are updated at least annually on policy developments.

All teachers are responsible for promoting and supporting safe behaviours in their classrooms and following school online safety procedures. Central to this is fostering a 'No Blame' culture so pupils feel able to report any bullying, abuse or inappropriate materials.

Key responsibilities of the Headteacher:

- Support safeguarding leads and technical staff as they review protections for pupils in the home and remote-learning procedures, rules and safeguards.
- Foster a culture of safeguarding where online safety is fully integrated into whole-school safeguarding
- Oversee the activities of the designated safeguarding lead and ensure that the DSL responsibilities listed in the section below are being followed and fully supported
- Ensure that policies and procedures are followed by all staff
- Undertake training in offline and online safeguarding, in accordance with statutory guidance and relevant Local Safeguarding Partnerships
- Liaise with the designated safeguarding lead on all online-safety issues which might arise and receive regular updates on school issues and broader policy and practice information
- Take overall responsibility for data management and information security ensuring the school's provision follows best practice in information handling; work with the DPO, DSL and governors to ensure a GDPR-

compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information
- Ensure the school implements and makes effective use of appropriate ICT systems and services including school-safe filtering and monitoring, protected email systems and that all technology including cloud systems are implemented according to child-safety first principles
- Be responsible for ensuring that all staff receive suitable training to carry out their safeguarding and online safety roles
- Understand and make all staff aware of procedures to be followed in the event of a serious online safeguarding incident
- Ensure suitable risk assessments are undertaken so the curriculum meets needs of pupils, including risk of children being radicalised
- Ensure that there is a system in place to monitor and support staff (e.g. network manager) who carry out internal technical online-safety procedures
- Ensure governors are regularly updated on the nature and effectiveness of the school's arrangements for online safety

All staff are familiar with the schools' Policy and will:

- Pay particular attention to safeguarding provisions for home-learning and remote-teaching technologies (see coronavirus.lgfl.net/safeguarding for an overview of safeguarding considerations for remote teaching technology. There are further details in the staff AUP.
- Recognise that RSHE will be introduced in this academic year and that it is a whole-school subject requiring the support of all staff; online safety has become core to this new subject
- Understand that online safety is a core part of safeguarding; as such it is part of everyone's job – never think that someone else will pick it up
- Read Part 1 of Keeping Children Safe in Education (whilst Part 1 is statutory for all staff, for SLT and those working directly with children, it is good practice for all staff to read all three sections).
- Read and follow this policy in conjunction with the school's main safeguarding policy
- Record online safety incidents in the same way as any safeguarding incident and report in accordance with school procedures.
- Understand that safeguarding is often referred to as a jigsaw puzzle – you may have discovered the missing piece so do not keep anything to yourself
- Notify the DSL if policy does not reflect practice in your school and follow escalation procedures if concerns are not promptly acted upon
- Identify opportunities to thread online safety through all school activities as part of a whole school approach in line with the RSHE curriculum, both outside the classroom and within the curriculum, supporting curriculum/stage/subject leads, and making the most of unexpected learning opportunities as they arise (which have a unique value for pupils)
- Whenever overseeing the use of technology in school or for homework or remote teaching, encourage and talk about appropriate behaviour and how to get help and consider potential risks and the age-appropriateness of websites (find out what appropriate filtering and monitoring systems are in place)
- When supporting pupils remotely, be mindful of additional safeguarding considerations.
- Carefully supervise and guide pupils when engaged in learning activities involving online technology, supporting them with search skills, critical thinking, age appropriate materials and signposting, and legal issues such as copyright and GDPR.
- Be aware of security best practice at all times, including password hygiene and phishing strategies.
- Prepare and check all online source and resources before using
- Encourage pupils/students to follow their acceptable use policy at home as well as at school, remind them about it and enforce school sanctions.
- Notify the DSL of new trends and issues before they become a problem so that action can be taken early.
- Take a zero-tolerance approach to bullying and low-level sexual harassment and any kind of harassment.
- Be aware that you are often most likely to see or overhear online safety issues (particularly relating to bullying and sexual harassment and violence) in the playground, corridors, toilets and other communal areas outside the classroom – let the DSL know.
- Receive regular updates from the DSL and have a healthy curiosity for online safeguarding issues

- Model safe, responsible and professional behaviours in their own use of technology. This includes outside the school hours and site, and on social media, in all aspects upholding the reputation of the school and of the professional reputation of all staff. More guidance on this point can be found in this Online Reputation guidance for schools.

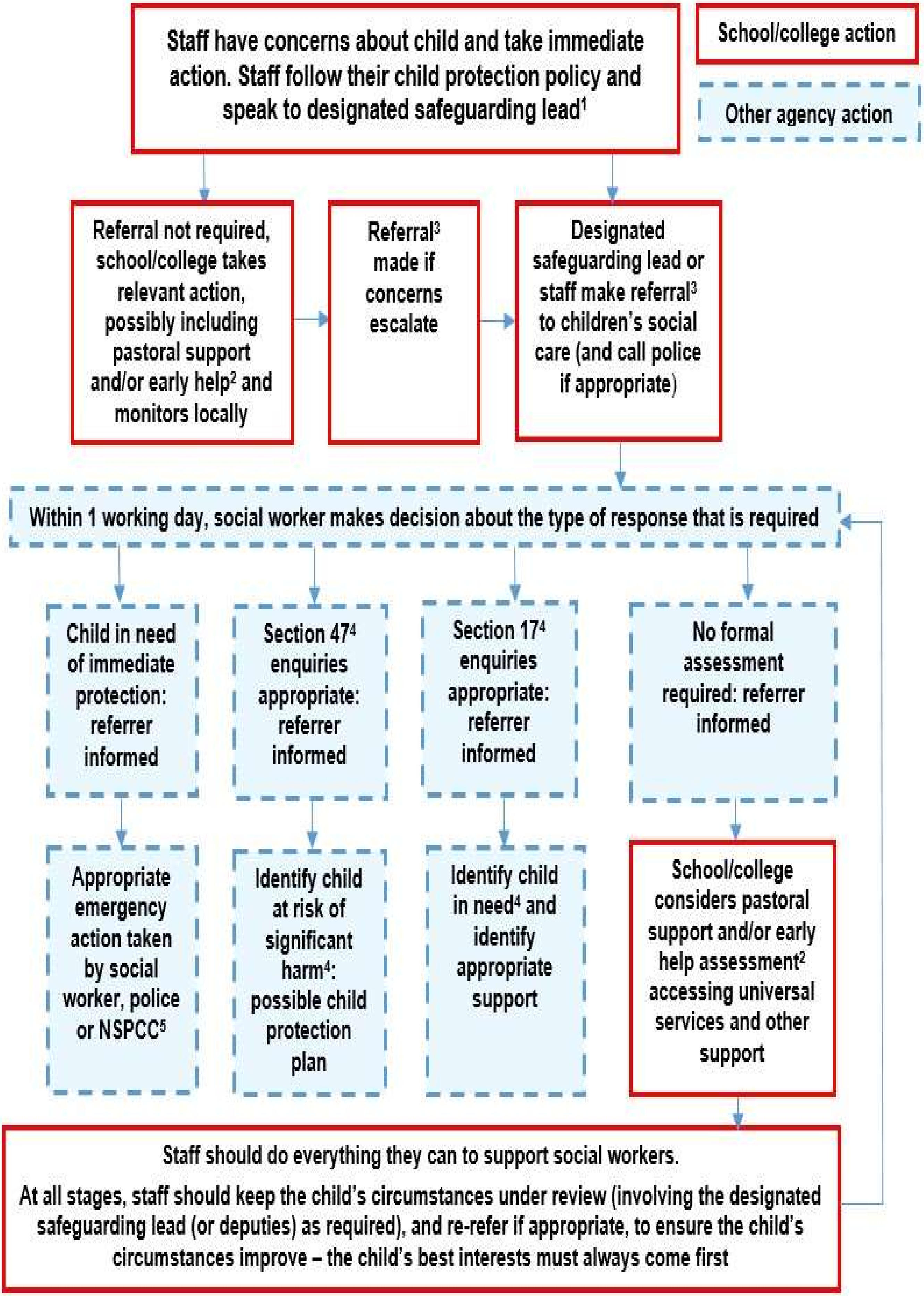
How will complaints regarding Online Safety be handled?

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

Staff and pupils are given information about infringements in use and possible sanctions. Sanctions available include:

- Interview/counselling by Headteacher and safeguarding lead
- Informing parents or carers;
- Removal of Internet or computer access for a period, [which could ultimately prevent access to files held on the system.
- Referral to LA / Police.
- Our online safety Coordinator acts as first point of contact for any complaint. Any complaint about staff misuse is referred to the Headteacher.
- Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy.
- Complaints related to child protection are dealt with in accordance with school / LA child protection procedures.

The following flow chart is taken from page 13 of Keeping Children Safe in Education 2020 as the key education-safeguarding document. As outlined previously, online safety concerns are no different to any other safeguarding concern.



School/college action

Other agency action

Staff have concerns about child and take immediate action. Staff follow their child protection policy and speak to designated safeguarding lead[1]

Referral not required, school/college takes relevant action, possibly including pastoral support and/or early help[2] and monitors locally

Referral[3] made if concerns escalate

Designated safeguarding lead or staff make referral[3] to children's social care (and call police if appropriate)

Within 1 working day, social worker makes decision about the type of response that is required

Child in need of immediate protection: referrer informed

Section 47[4] enquiries appropriate: referrer informed

Section 17[4] enquiries appropriate: referrer informed

No formal assessment required: referrer informed

Appropriate emergency action taken by social worker, police or NSPCC[5]

Identify child at risk of significant harm[4]: possible child protection plan

Identify child in need[4] and identify appropriate support

School/college considers pastoral support and/or early help assessment[2] accessing universal services and other support

Staff should do everything they can to support social workers.

At all stages, staff should keep the child's circumstances under review (involving the designated safeguarding lead (or deputies) as required), and re-refer if appropriate, to ensure the child's circumstances improve – the child's best interests must always come first

Using digital images and video safely Developing safe school web sites

The school website is an important, public-facing communication channel. Many prospective and existing parents find it convenient to look at the school's website for information and it can be an effective way to share the school's good practice and promote its work. Procedures and practice need to ensure website safety. A senior member of staff needs to oversee / authorise the website's content and check suitability. It should be clear who has authority to upload content into sections of the website. Having a website that is easy to maintain and update is helpful and many schools use one of the LGfL templates as a basis for this. This portal functionality is included within the broadband package.

Use of still and moving images

The school will take care when using photographs or video footage of pupils on the school website and will consider using group photographs rather than photos of individual children. First and last names of individuals in a photograph will not be used. This reduces the risk of inappropriate, unsolicited attention from people outside the school. The school will ensure that if a photograph or video is used that:

- If the photograph /video is used, we will avoid naming the pupil.
- If showcasing examples of pupil's work we will only use first names of pupils, rather than their full names.
- Only use images of pupils in suitable dress to reduce the risk of inappropriate use.

In many cases, it is unlikely that the Data Protection Act will apply to the taking of images e.g. photographs taken for personal use, such as those taken by parents or grandparents at a school play or sports day. However, photographs taken for official school use, which are likely to be stored electronically alongside other personal data, may be covered by the Data Protection Act. As such, pupils and students should be advised why they are being taken.

Parental permission should be obtained before publishing any photographs, video footage etc of pupils on the school website or in a DVD. This ensures that parents are aware of the way the image of their child is representing the school. A Parental Permission Form is an appropriate way of achieving this.

Procedures:

Use excerpts of pupils' work such as from written work, scanned images of artwork or photographs of items designed and made in technology lessons. This allows pupils to exhibit their work to a wider audience without increasing the risk of inappropriate use of images of pupils.

Links to any external websites should be thoroughly checked before inclusion on a school website to ensure that the content is appropriate both to the school and for the intended audience. Remember that the content of websites can change substantially, even in a short space of time. Check all links regularly, not only to ensure that they are still active, but that the content remains suitable too.

Text written by pupils will always be reviewed before publishing it on the school website. We will ensure that the work doesn't include the full name of the pupil, or reveal other personal information, such as membership of after school clubs or any other details that could potentially identify them. Although it may seem obvious, the school will check that pupils' work doesn't contain any statements that could be deemed defamatory.

The Headteacher is responsible for ensuring that the school's website does not infringe copyright or intellectual property rights through any content published. For example, using images sourced through Google, or using a Trademark for which copyright permission has not been sought or uploading educational content from educational websites/schemes of work.

If showcasing school-made digital video work, the school will ensure that pupils aren't referred to by name on the video, and that pupils' full names aren't given in credits at the end of the film.

Digital images, photographs and video clips can now readily be taken using mobile phones. Extreme abuse is the so called 'happy slapping' incidents sent to others or posted onto a website, e.g. a recent case of a posting on YouTube. It is therefore important to ensure that the risk of inappropriate use is minimised.

Staff are advised not to use their personal phone or camera without permission e.g. for a school field trip. If personal equipment is being used it should be registered with the school and a clear undertaking that photographs will be transferred to the school network and will not be stored at home or on memory sticks and used for any other purpose than school approved business.

Technical:
Digital images / video of pupils need to be stored securely on the school network and old images deleted after a reasonable period, or when the pupil has left the school.
When saving pictures, ensure that the image file is appropriately named. Do not use pupils' names in image file names or in <ALT> tag references when published on the web.
[An ALT tag is the HTML text describing a displayed image, used mostly for reasons of accessibility, since the tag can be voiced by screen readers]
Many schools are now using video as part of their Visual Literacy work. It is important that staff do not use software to 'rip-out' sections of copyrighted movies without permission.
There are safe online environments for publishing, such as the LGfL portal or Learning Platform and School 'Book Publishing' websites.
Education:

Ensure staff and pupils know who to report any inappropriate use of images to and understand the importance of safe practice. Staff and pupils also need to understand how to consider an external 'audience' when publishing or presenting work.

In this school:

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

- Uploading of information is restricted to the Headteacher, The Trust or the Business Support Manager
- The school web site complies with the school's guidelines for publications;
- Most material is the school's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status;
- The point of contact on the web site is the school address and telephone number. Home information or individual e-mail identities will not be published;
- Photographs published on the web do not have full names attached;
- We gain parental/carer permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter / son joins the school;
- Digital images /video of pupils are stored in the teachers' shared images folder on the network and images are deleted at the end of the year– unless an item is specifically kept for a key school publication;
- We do not use pupils' names when saving images in the file names or in the <ALT> tags when publishing to the school website;
- We do not include the full names of pupils in the credits of any published school produced video materials / DVDs;
- Staff sign the school's Acceptable Use Policy and this includes a clause on the use of mobile phones / personal equipment for taking pictures of pupils;
- Pupils are only able to publish to their own 'safe' web-portal on the LGfL in school;

- Pupils are taught to publish for a wide range of audiences which might include the SSC, parents or younger children as part of their ICT scheme of work;
- Pupils are taught about how images can be abused in their eSafety education programme;

How will e-mail be managed?

E-mail is now an essential means of communication for staff in our schools and increasingly for pupils and homes. Directed e-mail use in schools can bring significant educational benefits through increased ease of communication between students and staff, or within local and international school projects. However, un-regulated e-mail can provide a means of access to a pupil that bypasses the traditional school physical boundaries. The central question is the degree of responsibility for self-regulation that may be delegated to an individual. Once e-mail is available it is difficult to control its content.

Technology:

Incoming and outgoing e-mail can be restricted to approved addresses and filtered for unsuitable content and viruses. This is the first line of defense. Schools in London have an appropriate educational, filtered Internet based e-mail system through the London Grid for Learning (LGfL).
By default any pupil accounts that are created are automatically assigned as 'safe mail'. This means that they can only exchange e-mails with pupils and teachers from the same school. If a teacher wants to open up a class or a year group for a certain amount of time or permanently, they can do this by removing the safe mail restriction. This means that they would have a typical e-mail account that is able to send or receive e-mails with anyone.
All e-mails in the LGfL system go through a filtering process for inappropriate language regardless of whether they are in safe mail or not.
Where the school receives nuisance or bullying e-mails and the e-mail address of the sender is not obvious, it is possible to track the address using 'e-mail' tracking software.

Procedures:

In the school context, e-mail should not be considered private and most schools, and indeed Councils and businesses, reserve the right to monitor e-mail. There is a balance to be achieved between monitoring to maintain the safety of pupils and the preservation of human rights, both of which are covered by recent legislation.

All working in schools should avoid the use of personal e-mail addresses, such as Hotmail, and staff should be required to use appropriate LA or LGfL systems for professional purposes.
Individual pupil e-mails such as janet.brown@school.la.sch.uk which allow pupils to send and receive messages to and from the wider world, need to be carefully allocated to appropriate situations. Whole-class or project LGfL e-mail addresses can be used in primary schools, to communicate outside the school community.

Many teenagers or younger pupils will have their own e-mail accounts, such as the web-based Hotmail or G-mail, which they use widely outside school, usually for social purposes. If e-mail accounts are not monitored there is the risk that pupils could send or receive inappropriate material. External web-based e-mail accounts with anonymous names such as pjb354@emailhost.com make monitoring difficult. One strategy is to limit e-mail use to accounts on the school domain or even to limit pupils' e-mail to within the school network. Pupils are able to use their Google classrooms account under the direction of the class teacher during the school day. Teachers monitor the content of Google classrooms.

Education:

Pupils are taught about safeguarding, including online, through teaching and learning opportunities, as part of providing a broad and balanced curriculum. This may include covering relevant issues through personal, social, health and economic education (PSHE), assemblies, though the computing curriculum and through sex and relationship education (SRE).

Pupils need to be made aware of the risks and issues associated with communicating through e-mail and to have strategies to deal with inappropriate e-mails, which is part of the school's e- Safety and anti-bullying education programme.
There are programs that can be used with the youngest pupils that 'simulate' an E-mail system; this provides a useful environment to teach the skills of sending and receiving an e-mail with or without an

attachment to very young pupils.
Pupils need to understand good ‘netiquette’ style of writing, (this links to English) and appropriate e-mail behaviour appropriate to their age.

Managing the Internet Safely Why is Internet access important?

The Internet is an essential element in 21st century life for education, business and social interaction. ICT skills and knowledge are vital to access life-long learning and employment; indeed, ICT is now seen as a functional, essential life skill along with English and mathematics The statutory curriculum requires pupils to learn how to locate, retrieve and exchange information using technology including the Internet. All pupils should be taught to use the Internet efficiently and safely, and to develop a responsible and mature approach to accessing and interpreting information. The Internet can benefit the professional work of staff and enhances the school's management information and business administration systems. In support of this, the government provided a Standards Fund grant to support Local Authorities procures broadband services through local Regional Broadband Consortia (RBC). In London the London Grid for Learning (LGfL) is the RBC. All London schools are connected onto this broadband network. The LGfL is part of the National Education Network (NEN). All English maintained schools are expected to be part of the NEN.

The risks

The Internet is an open communications channel, available to all. Anyone can send messages, discuss ideas and publish material with little restriction. These features of the Internet make it both an invaluable resource used by millions of people every day as well as a potential risk to young and vulnerable people.

Much of the material on the Internet is published for an adult audience and some is unsuitable for pupils. In addition, there is information on weapons, crime and racism that would be more considered inappropriate and restricted elsewhere.

In line with school policies that protect pupils from other dangers, there is a requirement to provide pupils with as safe an Internet environment as possible and to teach pupils to be aware of and respond responsibly to any risk. This must be within a ‘No Blame’, supportive culture if pupils are to report abuse. Risks can be high outside school, so schools should consider extending an education programme to parents and carers.

Schools also need to protect themselves from possible legal challenge. The legal system continues to struggle with the application of existing decency laws to computer technology. It is clearly a criminal offence to hold images of child pornography on computers or to use Internet communication to ‘groom’ children. The Computer Misuse Act 1990 makes it a criminal offence to “cause a computer to perform any function with intent to secure unauthorised access to any program or data held in any computer”. Sending malicious or threatening e---mails and other messages is a criminal offence under the Protection from Harassment Act (1997), the Malicious Communications Act (1988) and Section 43 of the Telecommunications Act (1984).

Schools help protect themselves by making it clear to users that the use of school equipment to view or transmit inappropriate material is “unauthorized” and infringements will be dealt with; and by ensuring that all reasonable and appropriate steps have been taken to protect pupils. Reasonable steps include technical and policy actions and an education programme for pupils and staff, (and parents).

Technology:

Schools should be connected to the NEN through their RBC. In London this is the London Grid for Learning (LGfL) who procures the broadband supply from Synetrix. Across this schools’ fibre network, a range of services are provided. Internet filtering is a key service. This is updated and monitored by Synetrix working with their Third Party Suppliers. All London maintained schools should be part of this network.

Additionally, schools should have up-to-date anti-virus, anti-spyware and anti---spam ware software and approved firewall solutions installed on their network. There are LGfL solutions provided for all of these and should be set-up to be automatically updated so that networks remain up-to-date.

To make sure rogue applications are not downloaded and hackers cannot gain access to the school's equipment or into users' files through Internet use, staff and pupils should not be able to download executable files and software.

Unfortunately, inappropriate materials will inevitably get through any filtering system. So, schools should be vigilant and alert so that sites can be blocked. Conversely, sometimes appropriate websites need to be unblocked. In larger schools, network managers will be able to block or liaise directly with Synetrix over this. In primary or smaller schools, there should be a named member of
the ICT strategy team who manages the filtering policy for the school: this person may be the technician or the ICT coordinator, and the Trust will usually be able to provide them with advice and back-up.

By working together, London schools help to make the filtering system as effective as possible. Networks can have 'health' checks to ensure they have the latest versions of patches and service updates and to check speed and the possibility of having inappropriate applications on the network. Synetrix provide a service that schools can purchase.
Individual log-ins, coupled with Auditing software, means activity on the network can be monitored and logged. Security can be enhanced by 'timing-out' Internet or network sessions. High level monitoring of website access is also undertaken by Synetrix and logs can be obtained where a site is under investigation.

Within lessons, there is network 'remote' management software available on the market, which enables the 'tutor' / teachers to present only the software or the Internet links they want pupils to access for that lesson or topic – particularly useful for younger pupils. Your LA may be able to offer advice on such products.

Filtering, coupled with child-friendly search engines [e.g.http://yahooligans.yahoo.com/ | http://www.askforkids.com/] reduce the likelihood of children finding inappropriate materials. Schools should set-up search engines so that 'safe search' is turned on: Although not a child friendly search engine, it is worth noting that Google can be forced into safe search mode through the LGfL provision. Caching some sites so they are now essentially stored as off-line resources for viewing later from the Local Area Network (LAN) is another useful strategy.

Pupils publishing to the Internet on a class LGfL website removes the difficulties of pupils publishing on a publicly available Web site because this can be a safe, closed environment which only they will have access to via their username and password.

Schools should not send personal data across the Internet unless it is encrypted or sent via secure systems such as the DfES s2s site or an approved Learning Platform etc.

Staff are reminded not leave a computer or any other device logged in when they are away from their desk/working areas.

Online Safety

Anti-bullying and Cyber Bullying

We will seek to promote e-safety by:

- Assigning our Computing Lead to work in partnership with local authority, The Trust and external providers;
- Developing a range of procedures that provide clear and specific directions to staff and volunteers on the appropriate use of ICT;
- Supporting and encouraging the pupils to use the opportunities offered by mobile phone technology and the internet in a way that keeps themselves safe and shows respect for others;
- Supporting and encouraging parents/carers to do what they can to keep their children safe online and when using their mobile phones and game consoles;
- Incorporating statements about safe and appropriate ICT use into the codes of conduct both for staff and volunteers and for children and young people;
- Developing an online safety agreement for use with our pupils, parents/carers;
- Use our procedures to deal firmly, fairly and decisively with any examples of inappropriate ICT use, complaints or allegations, whether by an adult or a child/young person (these may include breaches of filtering, illegal use, cyber---bullying, or the use of ICT to groom a child or to perpetrate abuse);
- Informing parents and carers of incidents of concern as appropriate;
- Reviewing and updating the security of our information systems regularly;
- Providing adequate physical security for ICT equipment;
- Ensuring that user names, logins and passwords are used effectively;
- Using only official Avanti email accounts, and monitoring these as necessary;
- Ensuring that the personal information of staff, volunteers and service users (including service users' names) are not published on our website;
- Ensuring that images of children, young people and families are used only after their written permission has been obtained, and only for the purpose for which consent has been given;
- Any social media tools used in the course of our work with children, young people and families will be risk assessed in advance by the member of staff wishing to use them;
- Providing effective management for staff and volunteers on ICT issues, through supervision, support and training;
- Examining and risk assessing any emerging new technologies before they are used within the organisation.

Policy statement

This school:

- Maintains broadband connectivity through the LGfL and so connects to the National Education Network;
- Works in conjunction with the LA to ensure any concerns about the system are communicated to LGfL so that systems remain robust and protect students;
- Ensures network health through appropriate anti-virus software etc and network set-•up so staff and pupils cannot download executable files such as .exe / .com / .vbs etc.;
- Ensures their network is 'healthy' by having LA health checks annually on the network;
- Utilises caching as part of the network set-up;
- Ensures the Systems Administrator / network manager is up-to-date with LGfL services and policies;
- Ensures the Systems Administrator / network manager checks to ensure that the filtering methods are effective in practice and that they remove access to any website considered inappropriate by staff immediately;
- Never allows pupils access to Internet logs;
- Has network auditing software installed;

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

- Uses individual log-ins for pupils [from Y1/your choice] and all other users;
- Uses teacher ‘remote’ management control tools for controlling workstations / viewing users / setting-up applications and Internet web sites, where useful;
- Never sends personal data over the Internet unless it is encrypted or otherwise secured;
- Ensures pupils only publish within appropriately secure learning environments such as their own closed secure LGfL portal or Learning Platform.

Policy procedures for teaching and learning:

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. There is an expectation that a teacher or a learning support assistant is to be supervising computer use at all times. Pupils must not be left alone on any occasions with a computer/device unsupervised.

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. Of course the experienced teacher will choose a topic with care, select the search engine and then discuss with pupils sensible search words, which should be tested beforehand. Pupils do not need a thousand Web sites on weather. A small selection may be quite enough choice. Favourites are a useful way to present this choice to pupils. If teachers’ web site selections for various topics are put on the school web site, access by pupils from home and by other schools is made possible. There may even be difficulties here. Hackers can infiltrate a site or take over the domain, resulting in a previously acceptable site suddenly changing, for example, to a pornographic one. Therefore, sites should always be previewed.

Search Engines

Some common Internet search options are high risk, for example Google image search. Some LAs and Councils block this (at a Corporate level). 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 LA about this. LGfL guidance is available on the safety site.

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 podcasting (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. However, they are high-risk environments and it is essential that teachers use them carefully.

Video Conferencing

Webcams: are used to provide a ‘window onto the world’ to ‘see’ what it is like somewhere else. [e.g the LGfL nature cam and weather cams.] Webcams are also used widely across London for streaming video as part of a video conferencing project. Using the Click to Meet LGfL approved software; video conferencing provides a ‘real audience’ for presentations and access to places and professionals –

bringing them into the classroom. Synetrix provides a video conferencing service across the broadband network and it is managed by LGfL. LGfL has made an agreement with JVCS (the Janet Videoconferencing Service) to host calls. In order to create calls the school needs to register with JVCS and with the Click-to-Meet server. All conferences are therefore timed, closed and safe. Advice can be found from:www.vc.lgfl.net

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 school's 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. Social networking sites allow users to share and post web sites, videos, podcasts etc. It is important for children to understand that these sites are public spaces where adults hang out. They are environments that should be used with extreme caution and many carry a minimum age requirement. 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 such as GridClub SuperClubs. Additionally, the LGfL Learning Platform provides a safe environment for pupils to create their own web space, store files in an ePortfolio, and communicate with others through 'closed' discussions, etc.
Upskirting

It is important that everyone understands that upskirting (taking a photo of someone under their clothing) is now a criminal offence, as highlighted in Keeping Children Safe in Education and that pupils/students can come and talk to members of staff if they have made a mistake or had a problem in this area.

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.

Chat rooms

Many sites allow for 'real-time' online chat. Again, children should only be given access to educational, moderated chat rooms. The moderator (or referee) checks what users are saying and ensures that the rules of the chat room (no bad language, propositions, or other inappropriate behaviour) are observed. Pupils should be taught to understand the importance of safety within any chat room because they are most likely at risk out of school.

Sanctions and infringements

The school's Internet online safety / Acceptable Use policy needs to be made available and explained to staff / SSC members, pupils and parents, with all signing acceptance / agreement forms appropriate to their age and role.

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 referred at the earliest opportunity to the local police station. 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.

Policy statement

This school:

- Supervises pupils' use at all times, as far as is reasonable, and is vigilant in learning resource areas where older pupils have more flexible access;
- We use the pan-London LGfL filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature;
- Staff preview all sites before use [where not previously viewed and cached] or only use sites accessed from managed 'safe' environments such as the Learning Platform;
- Plans the curriculum context for Internet use to match pupils' ability, using child-friendly search engines where more open Internet searching is required;
- Is vigilant when conducting 'raw' image search with pupils e.g. Google or Lycos image search;
- Informs users that Internet use is monitored;
- Informs staff and students that that they must report any failure of the filtering systems directly to the [system administrator / teacher / person responsible for URL filtering]. Our systems administrators report to LA / LGfL where necessary;
- Blocks all Chat rooms and social networking sites except those that are part of an educational network or approved Learning Platform;
- Only uses approved Blogging or discussion sites, such as on the LGfL / approved Learning Platform and blocks others.
- Only uses approved or checked webcam sites;
- Has blocked pupil access to music download or shopping sites– except those approved for educational purposes such as LGfL's Audio Network;
- Requires pupils (and their parent/carer) from Key Stage 1 and 2, to individually sign an e- safety / acceptable use agreement form which is fully explained and used as part of the teaching programme;
- Uses closed / simulated environments for e-mail with Key Stage 1 pupils;
- Requires all staff to sign an online safety / acceptable use agreement form and keeps a copy on file;
- The Trust and proprietors ensure children are taught about safeguarding, including online, through teaching and learning opportunities, as part of providing a broad and balanced curriculum;
- 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;
- Keeps a record, e.g. print-out, of any bullying or inappropriate behaviour for as long as is reasonable online with the school behaviour management system;
- Ensures parents provide consent for pupils to use the Internet, as well as other ICT technologies, as part of the online safety acceptable use agreement form at time of their daughter's / son's entry to the school;
- Makes information on reporting offensive materials, abuse / bullying etc available for pupils, staff and parents;
- Filters and monitoring systems in place ensure this does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding;

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

Education programme:

It is a sad fact that pupils may occasionally be confronted with inappropriate material, despite all attempts at filtering and monitoring. Pupils need to know how to respond responsibly if they come across material that they find distasteful, uncomfortable or threatening. For example: to turn off the monitor and report the incident to the teacher or ICT manager for inclusion in the list of blocked sites.

Pupils must learn to recognise and avoid risks online– to become 'Internet Wise'. To STOP and THINK before they CLICK. Pupils also need to be 'savvy' about what they read, hear and see. In the same way that the quality of information received via radio, newspaper and television is variable, everyone needs to develop skills in selection and evaluation of Internet –based information. Just because something is published in text or on-line does not make it fact. It's therefore important that any education programme links to activities to help pupils evaluate what is fact, what is fiction and what is opinion, and that pupils consider whether something is plausible or biased.

Information literacy skills therefore need to be taught. These include skills to 'read' content– (contextual clues including design, lay-out, text, use of images, links to and from the content), where the material originates from and how the content can be validated. See the LGfL eSafety site has further guidance. More often in schools, pupils will be accessing reliable material but need to select that which is relevant to their needs, for instance to answer a homework question. Pupils should be taught research techniques including how to narrow down searches and how to skim and scan content.

The philosophy of sharing information across the Internet has increased the risk of pupils infringing copyright and committing Plagiarism (the theft of ideas and works from another author and passing them off as one's own). For older pupils, there are numerous 'essay bank' websites offering access to essays for free or for a fee, often encouraging students to submit their own works. Students should be aware of the issues around copyright and encouraged to look for copyright information on websites, so reinforcing their understanding of the importance this issue. They also need to be aware that plagiarism is not only cheating but where sufficient is copied, an illegal infringement of copyright also constitutes a criminal offence.

Pupils also need to understand the dangers of using unfiltered web access outside school at a location where parental controls or filtering have not been enabled. Pupils should be encouraged never to chat through a website or over a webcam with people that they do not already know and trust in the real world and not to post details about themselves to a website or in a Blog or message.

Pupils need to know how to deal with any Cyber Bullying incidents. Where they do communicate or publish work outside of the LGfL environment or other approved educational environment, it should be under adult supervision wherever possible.

Online safety must be built into schemes of work as appropriate, to ensure pupils are 'taught' safe behaviours and practice and the school must foster a 'No Blame' culture to ensure pupils feel able to report any abuse, misuse or inappropriate content. Key resources include the DfES/Becta Internet Proficiency Scheme at Key Stage 2 together with resources from CEEOP's Think U Know site.
Parents have an important role in supporting safe and effective use of the Internet by pupils– so schools need to consider a rolling training programme of support.

Policy statement

This school:

- Fosters a 'No Blame' environment that encourages pupils to tell a teacher / responsible adult immediately if they encounter any material that makes them feel uncomfortable;
- Ensures pupils and staff know 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;
- Has a clear, progressive online 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:

- Ensures all pupils and staff STOP and THINK before they CLICK
- Understands and expects a wider range of content on the internet, both in level and in audience, than is found in the school library or on TV;
- Supports pupils to discriminate between fact, fiction and opinion;
- Ensures pupils develop a range of strategies to validate and verify information before accepting its accuracy;
- Teaches pupils and staff skim and scan information;
- That both pupils and staff are 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;
- Ensures pupils and staff know some search engines / web sites that are more likely to bring effective results;
- Ensures that pupils and staff know how to narrow down or refine a search;
- Ensures pupils understand how search engines work;
- Ensures pupils understand how photographs can be manipulated and how web content can attract the wrong sort of attention;
- Ensures pupils understand 'Netiquette' behaviour when using an online environment such as a 'chat' / discussion forum, i.e. no bad language, propositions, or other inappropriate behaviour;
- To not download any files – such as music files --- without permission;
- Ensures that pupils understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, photographs and videos;
- Ensures pupils have strategies for dealing with receipt of inappropriate materials.

The school 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; Makes training available annually to staff on the online safety education program; Runs a rolling programme of advice, guidance and training for parents, including: Information in safety leaflets; in school newsletters; on the school web site; Demonstrations, practical sessions held at school;
Informs both pupils and parents about safe Internet use at home; Provides information about national support sites for parents.
Additional support materials can be found at: www.safety.lgfl.net

Filters and Monitoring

Keeping Children Safe in Education obliges schools to “ensure appropriate filters and appropriate monitoring systems are in place [and] not be able to access harmful or inappropriate material [but at the same time] be careful that “over blocking” does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding.”

At this school, the internet connection is provided by LGfL. This means we have a dedicated and secure, school safe connection that is protected with firewalls and multiple layers of security, including a web filtering system called WebScreen 3, which is made specifically to protect children in schools.

There are three types of appropriate monitoring identified by the Safer Internet Centre. These are:

Physical monitoring (adult supervision in the classroom, at all times)
Internet and web access
Active/Pro-active technology monitoring services

LONDON
GRID FOR LEARNING

AVANTI COURT
Excellence · Virtue · Devotion

Keeping safe: stop, think, before you click!
I have read the school ‘rules for responsible ICT use’. My teacher has explained them to me.

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

This means I will use the computers, Internet, e-mail, online communities, digital cameras, video recorders, and other ICT in a safe and responsible way. I understand that the school can check my computer files, and the Internet sites I visit, and that if they have concerns about my safety, that they may contact my parent / guardian.

Pupil’s signature

Parent/Carer’s Signature

Date: ______________