St. Philomena's Catholic Primary School

Headteacher: Miss V Maher

E-Safety Policy

2022

This policy should be read in conjunction with :-

Child Protection and Safeguarding Policy
Staff Code of Conduct
Policy for Managing Allegations against Staff
Anti-Radicalisation Policy
Safer Recruitment Policy

Home-School-Child Agreement

Date of Policy	**Signed**	**Position**
June 2022	Veronica Maher	Headteacher
Monitoring	**By**	**Date**
Reviewed	Resources Committee	
To be ratified	Full Governing Body	
Uploaded to website	**By**	**Date**
This policy will be reviewed **annually** by the full Governing Body Date of next review : June 2023		

Areas for improvement

Governor training
Breakdown of e-safety provision
Reporting and monitoring
Specified teacher training

Ofsted areas identified as requiring addressing:

1. Delivering online safety education to their pupils
2. Training
3. Policies, procedures and reporting
4. Leadership and good governance arrangements around online safety

Contents

1. Introduction and scope of the Policy

This policy seeks to formalise the management of E-safety risks, incidents, and education within the school. It relates to other policies including those for anti-bullying and safeguarding.

This policy should be read in conjunction with the school Safeguarding Policy, the Safeguarding Procedures (which incorporate the staff Code of Conduct), and the Anti-Bullying Policy. These detail the steps that should be taken in any safeguarding issue whether it is mediated by technology or not.

While many of the risks around E-safety will be familiar, modern technologies have created a landscape of challenges and dangers that are still constantly changing (including undue influence and radicalisation). The continued development of systems and devices mean that the school will need to be inventive and pragmatic in dealing with problems and threats as they emerge.

This E-safety Policy builds on government guidance. It applies to all members of the school community including staff, students/pupils, volunteers, parents/carers, and visitors. It also includes Early Years Foundation Stage.

1.1 *The nature of E-safety*

In the past, access to the internet was unusual. School computers would have been a rare opportunity for pupils to access it. Under these circumstances, it was then appropriate to make school systems into an electronic "walled garden" where filtering provided the virtual walls and little that was threatening could be seen by pupils.

Technology has, of course, moved on. Pupils and staff may now use a number of networks and a range of devices during a single day and each may have different levels of access and capability.

Nevertheless, St Philomenas believes that schools should be safe environments for learning. We judge the safeguarding of pupils both inside and outside of school to be of the highest priority and therefore we adhere to the following principles:

- The highest standards of technological protection are included as part of school networks.
- Pupils are taught about E-safety in all its aspects as part of the curriculum and E-safeguarding is seen as a responsibility of all staff.
- The school regards E-safety education as an important preparation for life.
- The school recognises that pupil and family information is sensitive and private. Data protection is regarded as a high priority.

1.2 *Assessing risks*

The school will take all reasonable precautions to ensure that users abide by the acceptable use rules and access only appropriate material.
The school cannot be liable for the consequences of staff or pupils deliberately breaking the acceptable use rules which are published for their protection.
Due to the international scale and linked nature of internet content, it is also not possible to guarantee that unsuitable material will never appear on a computer even when filtering is in place and users abide by the rules.

The school cannot accept liability for material accessed, or any consequences of internet access.

Staff using IT equipment will mainly be covered by the provisions of the Display Screen Equipment (DSE, Health and Safety) regulations 1992.

The use of DSE by pupils is not covered by the Display Screen Equipment Regulations. However it is good practice to apply the requirements of the legislation to their workstations thus helping them to develop safe working practices.

If pupils are issued with new IT equipment. guidance on how to use it safely will be given.

2. Systems and Procedures

2.1.1 *Responsibilities and duties*

The school will identify a member of staff to co-ordinate E-safety. This may be the designated Safeguarding Lead as the roles overlap. However E-safety is seen as a whole-school issue, and different members of staff will have responsibilities as listed below.

Headteacher	• To take overall responsibility for E-safety provision. • To take overall responsibility for data and data security (SIRO). • To be responsible for ensuring that staff receive suitable training to carry out their E-safety roles and to train other colleagues, as relevant. • To be aware of procedures to be followed in the event of a serious E-safety incident. • To oversee the staff acceptable use arrangements and take appropriate action over staff who breach them.

E-safety Co-ordinator	• To take day to day responsibility for E-safety issues and take a leading role in establishing and reviewing the school E-safety policies / documents. • To promote an awareness and commitment to e-safeguarding throughout the school community. • To ensure that E-safety education is embedded across the curriculum • To liaise with school IT technical staff. • To facilitate training and advice for all staff. • To be the main point of contact for pupils, staff, volunteers and parents who have E-safety concerns. • To ensure that all staff are aware of the procedures that need to be followed in the event of an E-safety incident. • To ensure that an E-safety incident log is kept up to date • To ensure that the SLT are regularly updated in E-safety issues and legislation, and to be aware of the potential for serious child protection issues that arise from (for example) ○ sharing of personal data ○ access to illegal / inappropriate materials ○ inappropriate on-line contact with adults / strangers ○ cyber-bullying
Network Technician	□ To report any E-safety related issues that arises, to the E-safety coordinator.
	• To ensure that staff users may only access the school's networks through an authorised and properly enforced password protection policy. • To ensure that provision exists for misuse detection and malicious attack (e.g. keeping virus protection up to date). • To ensure the security of the school IT system. • To ensure that access controls / encryption exist to protect personal and sensitive information held on school-owned devices. • The school's policy on web-filtering is applied and updated on a regular basis. • To ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster.
Data Manager	• To ensure that the school is compliant with all statutory requirements surrounding the handling and storage of information. • To ensure that any recording, processing, or transfer of personal data will be carried out in accordance with the Data Protection Act 1998. • To keep an up to date record of those granted access to school systems.

Teachers	• To embed E-safety issues in all aspects of the curriculum and other school activities • To supervise and guide pupils carefully when engaged in learning activities involving online technology(including, extra-curricular and extended school activities if relevant) • To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws.
All staff	• To read, understand and help promote the school's E-safety policies and guidance • To be aware of E-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices • To report any suspected misuse or problem to the E-safety coordinator • To maintain an awareness of current E-safety issues and guidance e. g. through CPD • To model safe, responsible and professional behaviours in their own use of technology • To ensure that any digital communications with pupils should be on a professional level and only through school based systems, never through personal mechanisms, e. g. email, text, mobile phones etc. • To ensure that all data about pupils and families is handled and stored in line with the principles outlined in the Staff AUP.
External groups	□ Any external individual / organisation will sign an Acceptable Use Policy prior to using any equipment or the Internet within school
Computing Curriculum Leader	• To oversee the delivery of the E-safety element of the Computing curriculum. • To liaise with the E-safety coordinator regularly.

2.2 Using School Systems

2.2.1 Conditions of using for School Systems

- All staff at the school sign an Acceptable Use Agreement (AUA) as part of their contract of employment. It details how school equipment and connections may be used.
- Pupils have combined Acceptable Use Agreements and E-safety guidance provided as three age-appropriate leaflets or posters. Although not a legal contract, it does set out what is expected by the school and this guidance is shared with parents.
- A separate register of when pupils were given (and agreed to abide by) the provisions of the agreement is kept for future reference with the pupil's records.

2.2.2 Staff use of Equipment and the Internet

The equipment provided for staff is primarily intended to support the teaching and learning of pupils. However, it is unreasonable to deny staff access to the internet for legitimate personal use (for example to contact a son or daughter’s school). Nevertheless, discretion and the highest professional standards are expected of staff using school equipment.

Expectations are set out in the Acceptable Use Agreement for staff mentioned above, but will include:

- Keeping a proper professional distance e. g. Not “friending” pupils or parents on social networking sites.
- Being aware of the need for appropriate language and behaviour particularly when using messaging or e-mails.
- Not posting inappropriate material on websites which can be viewed by pupils or parents.

2.2.3 *Using non-School Equipment –“Bring Your Own Device”*

Under some circumstances, both teachers and pupils are now able to use their own equipment in school and connect to the available network. This is normally called “bring your own device” (BYOD). Whether as staff member or pupil, it will be made clear to the user that the rules and expectations surrounding online behaviour remain in force regardless of the ownership of the equipment being used.

2.2.4 *AUA confirmation, and monitoring*

All staff members are required to sign an Acceptable Use Agreement (AUA) as part of their contract of employment. They have a dedicated log-on which requires them to use a strong password for access to the system.

Because of the age of the children, the use of a generic log-on is more appropriate for class management reasons.

- System monitoring is undertaken on a needs basis. For example if concerns about contacts between pupils are raised, then a record of messages can be retrieved by LGfL. Likewise, reports can be generated about the types of sites being accessed by users of the system and the number of times they have been requested.
- The E-safety Co-ordinator keeps a log of all E-safety incidents in the school and shares this on a regular basis with the senior leadership team and school network manager. He/she also monitors the implementation of the E-safety Policy and ensures that its provisions are working.

2.2.5 *Visitor access to the school internet*

- Visitors to the school can be given access to the internet by connecting to the wireless system. The filtering and monitoring systems apply as above.
- Access is only provided if the visitor signs a disclaimer which outlines restrictions and expectations of use.
- Access is provided under the general terms and conditions of the agreement which prohibits the sending or receiving of materials which “are offensive, abusive, defamatory, obscene, or menacing” or which are illegal.

2.3 Staying safe and informed

2.3.1 *Filtering protection*

The school relies on the filtering provided by its connection to the London Grid for Learning. This filtering is biased towards education and is approved by the Safer Internet Foundation. The browsers are also set to default to Google where the "safe browsing" features are locked to "on".

The filter is configurable to allow staff to access particular resources when needed, particularly those providing video and film clips. **Staff should be aware that if they relax the filter to allow a lesson to take place, then it should be reset afterwards**.

In a check of the filtering as part of Safeguarding in March 2017, a number of points emerged and this is set as guidance in the appendix to this policy.

2.3.2 *Staff and Governor training and updating*

- All staff will have E-safety training included as part of their safeguarding induction to the school. □ All staff will receive regular training in safeguarding pupils. E-safety is included as part of this. Staff members will receive training in specific elements of E-safeguarding (e. g. self harm) or a wider update at least once per year.
- E-safety incidents and concerns will be included under safeguarding issues at all staff briefings.
- There will be governor training in e-safety as part of the induction process and whenever the head teacher judges there to be a need under the governor training programme.

2.4 School Website

Advice, guidance, and links are available through the school website for parents and pupils. This advice includes details of how to report a problem to the school, and which members of staff have responsibility for resolving a problem or taking issues further. The school will also look towards introducing an anonymous reporting system which will enable anyone with a concern to share it with the school easily and directly.

2.5 Misuse and complaints

2.5.1 *Misuse of School Systems*

Because the Staff Acceptable Use Agreement is part of the contract of employment, misuse is a disciplinary matter. Pupil misuse (for example the sending of bullying messages to another pupil) can result in the withdrawal of facilities or further sanctions in line with the school's disciplinary policy. (However it should be said that this is rare and that most experiences within the school are entirely positive.) Abuse of the systems by visitors will result in the immediate withdrawal of access and possible further actions depending on the nature of the misuse.

2.5.2 *Handling E-safety complaints*

Complaints about IT misuse by pupils will be dealt with by a senior member of staff under the procedures of the school and according to the nature of the complaint.

Any complaint about staff misuse must be referred to the Head Teacher.

Complaints of a child protection nature must be dealt with in accordance with statutory child protection procedures. Pupils and parents will be informed of the school's complaints procedure.

3. Safeguarding and IT

3.1 *Reporting of E-safety concerns*

The school will always take reports concerning E-safety very seriously. The school will take appropriate action dependent upon the nature of the concern raised. All incidents that come to the attention of school staff should be notified to the E-safety co-ordinator.

The E-safety Co-ordinator will ensure that pupils, parents, volunteers, and staff understand that they can contact them with concerns at any time.

Any incident that raises wider questions of safeguarding will also be communicated to the Designated Safeguarding Lead(s) as soon as possible and action under the Safeguarding Policy and Procedures will be considered.

3.2 *Particular circumstances for concern:*

Inappropriate material appearing on school computers

- Pupils are taught that they are not at fault if they see or come across something online that they find worrying or upsetting. If they share their experience, then it is something that the teacher and the rest of the class can learn from. The teacher should report the incident to the E-safety co-ordinator who will log the problem and liaise with the network manager to adjust filtering settings.

Abusive messages on school computers

- Pupils who receive abusive messages over school systems will be supported, and advised not to delete messages. The E-safety co-ordinator will be informed and an investigation begun initially with the help of LGfL and the IT support providers.

Parental reporting of bullying/pressure

- Parents may become aware that their child is suffering from bullying or other pressures originating in the school but continued via electronic means. Parents should know that the school encourages parents and pupils to approach them for help, either via the class tutor or directly to the head teacher. A full discussion of Cyber bullying, and the actions which may be taken is included in the school Anti-Bullying Policy and Procedures document.

Pupil disclosure of concerns or abuse

- For many reasons, a pupil may choose to disclose a concern to a member of school staff. The situations leading to a disclosure can range widely, from a general worry to long-term abuse, and for this reason Safeguarding Training for all staff is essential so that situations or concerns are dealt with appropriately. A disclosure should always be passed on to the Safeguarding Lead and, where appropriate, the E-safety co-ordinator.

Pupil reporting outside of school

- Pupils will be taught that if something worries them, or if they think a situation is getting out of hand, that they should share this with their parents, and consider using the online **Report CEOP** button to make a report and ask for help.

4. E-safety Teaching and Pupils

4.1 Teaching E-safety in School

The school curriculum includes lessons and activities in E-safety for all pupils.

The intention is to develop pupils' **awareness**, **resilience**, and **skills** in the wider electronic world. Pupils will explore issues such as:

- **Persuasion and reliability** (internet scams, phishing, unreliable information, radicalisation, etc.)
- **Personal information and safety** (sexting, social network information, personal images, etc.)
- **Sexual exploitation** (grooming, "offender not present" activities, etc.)
- **Online bullying** (text abuse, “trolling”, etc.)

The activities are differentiated with regard to age (younger pupils are provided with materials which have simpler vocabulary and concepts).

The curriculum is varied and may comprise:

- staff-led skills sessions (eg How to configure *Facebook* privacy settings),
- whole school assemblies led by older pupils, and other examples of peer mentoring,
- discussion groups,
- Safer Internet Day activities, □ formal lessons.

Importantly, the teaching covers not only what the problems are, but how to deal with and avoid them. Wherever possible, we will engage older pupils to share their experiences and advise others about personal safety and responsibility online.

These activities and lessons will be part of the Computing/IT and PSHE schemes of work.

The E-safety co-ordinator will keep up to date on emerging trends and alter the guidance and focus of the curriculum to suit.

4.2 Using web sites with pupils

Pupils are often directed to internet sites as part of their work in school. Many of these sites are very useful and provide facilities such as creating presentations, or working with recorded sounds. In a rapidly changing electronic world it is impossible to ask permission from parents for every new site that might be used with pupils or that pupils might discover for themselves. Instead the school will abide by the following principles:

- All sites will be filtered via the LGfL system to minimize the risk of inappropriate material being accessed.
- If pupils are asked to make online accounts for access to materials, the minimum of identifiable personal information will be disclosed and only school e-mails will be used.

- The school will be as open as possible about the sites and software it uses and welcome parents who wish to raise concerns or understand more about the way that IT contributes to education.

It should be noted that because of differing laws (particularly in the USA) terms and conditions of some sites have apparent restrictions which do not apply in the UK. The school takes the view that "restricted" but innocuous sites with useful educational materials will be used unless concerns become evident.

4.3 *Creating online work and websites*

Pupils may create pieces of work which are not stored within the school controlled servers. This might include creating simple websites. However the following conditions will always be followed:

- Websites created will not feature personal information or images. The content will always be educational (eg. countries of the world) and not personal.
- Whenever possible, online work will always be password protected.
- Work will not be uploaded to freely available "public" sites.

4.4 *Pupils using e-mail and other messaging systems*

- When using the school system, pupils may only use approved email accounts.
- Pupils must immediately tell a member of staff if they receive offensive email.
- Pupils must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission.
- As part of the guidance and e-safety notes, pupils undertake to never send hurtful or damaging messages to anyone in the school community regardless of the ownership of the device that the message is sent or received on. Older students will be reminded that the sending of abusive messages is illegal.

5. Risk Management – Everyday E-safety

5.1 *Publishing Staff &Pupil Information and Photographs*

The school website

The contact details on the website should be the school address, email and telephone number. Staff or pupils' personal information will not be published. The Head Teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

5.2 *Publishing pupils' images and work on the web*

Open / public sites

The school understands that public sites can be used to gather information and the locations of pupils. Written permission to use photographs and work on websites will have been obtained as part of the contract signed by parents. However, unless there is need to identify a pupil (e. g. to celebrate a prize) the following guidelines should be observed:

- Pupils' full names will not normally be used on the website or blog, particularly in association with photographs.

- Photographs published on the website, or elsewhere that include pupils will be selected carefully. Care will be taken when taking digital / video images that pupils are appropriately dressed.

Closed/ Secure sites

Pupils' images, video, and work, can be made available to parents on secure areas of the web as long as the following measures are adhered to:

- The parents /carer should have a secure log-on to view the information on their pupils.
- Parents should be made aware that their child's images may be included in group work viewable by other parents /carers.

5.2 Managing emerging technologies

- Emerging technologies will be examined for educational benefit and the risks will be assessed. It should be realised that potential problems or harm may not emerge until after the adoption of a technology.
- The senior management of the school (including the E-safety co-ordinator) will reassess the suitability of technology and systems over time and check that they remain suitable, secure, and effective.

6 Communicating the Policy

6.1 Introducing the E-safety Policy to Children

- Each pupil in KS2 will have a personal copy of the school's E-safety and acceptable use leaflet.
- Versions of the E-safety / Acceptable Use rules will be posted in all networked rooms and discussed with pupils as needed. The aim will be to keep the policy familiar and fresh for pupils rather than as something which is only referred to at odd times.
- Pupils in the KS1 will have a copy of the e-safety wall poster in their room and it will be referred to regularly by teachers.
- Pupils will be informed that network and internet use will be monitored.
- By signing the Home-School-Child Agreement, pupils make a commitment to following all school rules including those concerning safe use of the internet.

6.2 *Staff and the E-safety Policy*

- All staff will be given a copy of the E-safety Policy and its importance explained.
- They should sign a copy of the Staff Acceptable Use agreement as part of the contract of employment.

Staff should be aware that internet traffic can be monitored and traced to the individual user. Because of this, discretion and professional conduct is essential in school.

6.3 Communicating E-safety information to parents

- As already mentioned, the school website will give information on E-safety and how the school can help.
- E-safety advice will be included as a regular feature in newsletters and as part of the ongoing dialogue between home and school.
- The school will hold E-safety events to brief parents about E-safety developments and policies on an occasional basis often as part of events such as Safer Internet Day.
- Wider information events for parents will have E-safety items included in the programme.

E-safety - Sources of information and guidance

Resources for pupils, parents, and teachers	
Think you know https://www.thinkuknow.co.uk/	A premier site for resources and activities across the age ranges. This is linked to CEOP and is still one of the best places to look for resources and guidance.
CBBC Stay Safe Pages http://www.bbc.co.uk/cbbc/topics/stay-safe	A collection of games, quizzes and activities about E-safety in general. Very visual and engaging.
Childnet International http://www.childnet.com/	One of the first organisations to promote internet safety. Their SMART rules are written into the school guidance for pupils. The site has lots of information and activities with more of a emphasis on Junior and infant pupils (eg DigiDuck)
DfE Advice for Parents and Carers on Cyberbullying https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/444865/Advice_for_parents_on_cyberbullying.pdf	2014 advice with links to lots of other areas including ThinkUKnow. Very useful

Digizen http://www. digizen. org/	A Childnet project about digital citizenship. Looking slightly out of date now, but with some useful ideas, activities, and videos.
Digital Literacy guidance and teaching materials Professor Alan November http://novemberlearning. com/educational-resources-foreducators/information-literacyresources/	These invaluable resources can be used to teach young people • Not to believe everything that is on the web • How to check where information is coming from □ How to "read" web resources Some useful links to other teaching and "spoof" sites such as the North West Tree Octopus.
Ten Tips for Using Facebook http://www. broadwayacademy. co. uk/wpcontent/uploads/2014/07/Facebook. pdf	This PDF resource is published by Broadway Academy in Birmingham. It offers safety tips and then reasons why they are a good idea. It would make a good starting point for a lesson with senior pupils.
Beat Bullying http://www. beatbullying. org/	An independent organisation that works inside and outside of schools to develop young people as cybermentors. These mentors then help more marginalised students cope with bullying issues.
NSPCC – Online safety http://www. nspcc. org. uk/help-and-advice/forparents/onlinE-safety/onlinEsafety_wdh99554. html	Materials on a number of areas including sexting, and cyber bullying. Well worth a look.

Guidance and information for school managers, leaders and others.	
CEOP http://ceop. police. uk/	Child Exploitation and Online Protection Centre. Now a section of the National Crime Agency, CEOP is less active than in the past, but still a mainstay of training and resources.

Get Safe Online https://www.getsafeonline.org/	A good "expert" site part-funded by the UK Government which covers a wide range of issues from technical to social. Really comprehensive and a good place to think about the issues and get information.
UK Safer Internet Centre. http://www.saferinternet.org.uk/	This a site which amalgamates information and links from Childnet International, South West Grid for Learning, and the Internet Watch Foundation. This is where the UK Safer Internet Day is promoted and organised. Well worth a look.
London Grid for Learning http://www.lgfl.net/esafety/Pages/safeguarding.aspx	Although LGFL's main purpose is to link state schools across London, their E-safety resources are open to all and are quite exceptional. They include sample school policies, links to audit tools, and Ofsted expectations. Not everything is recent, so it is wise to pick and choose, but still excellent.
DfE Cyberbullying: Advice for Head Teachers and school staff. 2014. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/374850/Cyberbullying_Advice_for_Headteachers_and_School_Staff_121114.pdf	Non-statutory guidance on what staff should do to minimise their exposure to abuse, and what can be done if an incident occurs.
South West Grid for Learning http://www.swgfl.org.uk/home	Like the LGfL, this is one of the original broadband consortia for schools. However, they have developed a suite of audit tools and E-safety training services which schools can buy into or use by registering. The 360 Degree Safe audit is liked by a number of schools.
Internet Watch Foundation **https://www.iwf.org.uk/**	The industry organisation for the reporting and removal of UK based illegal and abusive material on the web. Contains a reporting form and guidance on various forms of content. It has no jurisdiction outside of the UK but will pass on information to appropriate authorities.

Digital Awareness UK **http://digitalawarenessuk.com/about/**	A company which uses young internet professionals to advise schools and pupils on their online presence.
UK Council for Child Internet Safety (UKCCISS) https://www.gov.uk/government/groups/uk-council-for-childinternet-safety-ukccis	UKCCISS is a para-governmental body that brings together a very wide range of partners from within industry, academia, and education to look over the changing landscape of technology and what this means for children. A good source for digests of the latest research and ideas in this area.

Guidance with a more technical bias	
Microsoft Safety Center http://www. microsoft. com/en-gb/security/familysafety/default. aspx#Internetuse	This is a text-based list of things that families could/ should do online. A little obvious and worthy perhaps, but still sound and with links to Microsoft OS tools for taking control of access and denying unwanted sites.
Norton Anti- Virus blog /guidance http://community. norton. com/blogs/norton-protectionblog	Norton's blog, is more than an advertising vehicle and contains information on new scams and threats as they arise together with technical and non-technical ways to protect yourself.
Google Safety https://www. google. com/safetycenter/#home	This is a set of tools to try and make the most popular of search engines more family friendly. Amongst other things it sets out how to select "safe search" on a browser and then lock it. (However a personal test of "safe search" suggests that it cannot be totally effective. It isn't a panacea.)
OFCOM – Guidance on Parental Controls for Games Consoles http://consumers. ofcom. org. uk/internet/onlinE-safety-andsecurity/parental-controls-forgames-consoles/	Very useful advice on internet-connectable devices and how they can be managed. They also have information on mobile phone usage. HOWEVER, beware of the links to a site called "Chatdanger" which is not information or education but now appears to be links to explicit chat sites.

Netlingo www. netlingo. com/emailsh. cfm	An online dictionary of “text chat” for decoding conversations. Often enlightening and sometimes verging on the poetic. . . The problem is that subgroups make and use acronyms all the time and they go in and out of fashion. What may be commonly understood in Sydenham may be unheard of in San Diego. . .

Appendix 2

Staff ICT Acceptable Use Agreement

I understand that working in an educational context brings with it high expectations of behaviour and integrity, and responsibilities with regard to safeguarding. These expectations include:

- Interacting with pupils in an appropriate way.
- Interacting with colleagues, parents, and other school or work contacts in an appropriate way.
- Being trustworthy with confidential and sensitive information.
- Looking after the fabric and equipment of the school, and respecting school property.
- Maintaining the reputation of the school (even when not at work).
- Maintaining professional standards of conduct.

These things are equally true when IT systems, including computers and phones, are involved. ***Staff may use school equipment/network for:***

- School/work purposes.
- Reasonable personal use that does not interfere with work. ***I understand:***
- This agreement applies to the use of school IT systems regardless of location.
- There is a presumption that emails, voice messages and data are stored on school equipment for business purposes. This information will be filtered and monitored, and may be accessed to meet business needs.
- Whilst the school does not prohibit staff interacting with parents on social media, it is not encouraged.

I will not:

- Do anything that may compromise the safety of children or staff.
- Disclose my username or password to anyone else.
- Try to use any other person's username and password for any purpose.
- Do anything offensive that might bring the school into disrepute.
- Access, copy, remove or alter any other user's files without their explicit permission. □ Engage in any on-line activity that may compromise my professional responsibilities.
- Attempt to install programmes on a machine, or store programs on equipment unless approved by school management.
- Try to circumvent security settings or content filters. □ Deliberately breach anyone's copyright.

I will:

- Bring to the attention of a member of the Senior Leadership Team any IT activity or material that may be inappropriate or harmful.
- Report any damage or faults involving equipment or software, however, this may have happened, as soon as reasonably possible.
- Only use chat and social networking sites in accordance with the school's policies.
- As far as is possible, use LGFL mail, work phones, and other school communication systems to communicate with pupils. I will only use personal phones or email where the use of school systems would be impractical, and I will never communicate with pupils using my personal social media accounts. At all times, I will observe the guidelines on acceptable behaviour contained in the safeguarding procedures in order to avoid comment or speculation.

- As far as is possible, use school-provided systems to communicate with parents on school and pupil matters. I will maintain professional standards of conduct if I communicate with parents socially using personal phones, email or social media. ***Information Security***

I understand that I may have access to sensitive information about colleagues, families or pupils in our care. I will comply with the school guidance on data protection and will keep sensitive information secure. I will not send sensitive information via personal email accounts (Hotmail, GMail etc) or store it on:

- Un-encrypted USB sticks
- Personal devices (phones, laptops) or
- Personal 'Cloud storage' (Dropbox, iCloud)

Images & Videos

In order to prevent allegations of inappropriate activities, including against EYFS staff, I will not store images of pupils on my personal devices. Any images taken on personal devices will be downloaded to school systems as soon as reasonably possible and the personal copy permanently removed.

Bringing Your Own Device

When I use personal devices in work, I understand that the same expectations of behaviour apply as if I were using school equipment.

I understand that if I fail to comply with this Acceptable Use Agreement, I may have my IT access suspended and/or be subject to disciplinary action. A copy of this agreement is available upon request.

I understand a copy of this signed document will be placed on my personal file.

I have read and understand the above.

Staff / Volunteer Name □

Signed □

Date □

Web filtering and pupils - Advice

The school receives its internet connection via the London Grid for Learning. LGfL is a long-established organisation who work with London schools. They apply filters to the content that we can receive. The software used is called **WebScreen 2** and is a filtering system approved by the UK Safer Internet Centre. It has an education bias and more information can be found here: https://www.lgfl.net/downloads/online-safety/LGfL-OS-Appropriate-Filtering-for-EducationSettings-Provider-Response-June-2016.pdf.
However it is not completely foolproof and the reasons for this are linked with the nature of the internet itself. Some examples:

YouTube is blocked and has to be released for a teacher to use educational resources. However- if a YouTube video is embedded in another site which is innocuous (e.g. a news site) then the video will play and it will include whatever graphic content the original contained.

Google Image Search - It is possible that an educational project on (say) birds might prompt children to use innocuous search terms such as great tit, shag, etc. However the image search may bring up very explicit 'thumbnail' images. These thumbnails cannot be filtered, although the website links that would take you to the sites certainly would be. Google Safe Search is locked "on" to reduce the problem, but it will not eliminate it.

Commercial selling sites (eg Amazon) may contain examples of extremely graphic sex toys and "aids". These are not filterable since they are contained within a general site which includes millions of other items.

Dealing with inappropriate things that appear on pupils screens….

- Teachers should be aware that they need to be vigilant when using web-based resources. We cannot completely rely on the filtering. There should not be unsupervised "free roaming" allowed in school, whatever is deemed acceptable at home.
- Teachers and other staff should quickly intervene if they believe that inappropriate items have appeared. The action they take will depend on the nature of the material and the age of the pupils involved. It may mean simply turning off a screen or closing a laptop and dealing with the content when the children have left the room. However, it may be appropriate to use the material to begin a discussion of what to do when they come into contact with radicalisation / extreme sexual / violent material outside of a school context. **The professional judgement of the teacher is key. They should inform the headteacher of the incident and any action that they have taken.**
- If an unacceptable website has slipped past the filters, it can be removed manually from the list of approved sites. Please note the website name/address and inform the office who will ask a designated LGFL contact to remove it.