E-SAFETY AND ACCEPTABLE USE POLICY
for pupils in relation to computing, mobile phones and other electronic devices

Date policy reviewed:	14 January 2020
Date of next review:	14 January 2022
Person(s) responsible for review:	SLT (VF)

CONTENTS

This policy consists of three sections:

SECTION A - General

1. COMPUTING IN THE CURRICULUM

Technology has transformed the entire process of teaching and learning at The Manor Preparatory School. It is a crucial component of every academic subject, and is also taught as a subject in its own right. Our classrooms are equipped with electronic whiteboards, projectors and computers. In addition to our ICT suites we have a number of full class sets of chromebooks, laptops and iPads available for use by the pupils. Computer and internet use is always supervised by an adult.

All of our pupils are taught how to research on the internet and to evaluate sources. They are educated into the importance of evaluating the intellectual integrity of different sites, and why some apparently authoritative sites need to be treated with caution. Some sites that appear to be serious, impartial, historical sites, actually masquerade as sources of racist, homophobic, jihadist or other propaganda. Some free, online encyclopedias do not evaluate or screen the material posted on them.

2. THE ROLE OF TECHNOLOGY IN OUR PUPILS' LIVES

This communications revolution gives young people unrivalled opportunities. It also brings risks. It is an important part of our role at The Manor Preparatory School to teach our pupils how to stay safe in this environment and how to avoid making themselves vulnerable to a range of risks, including identity theft, bullying, harassment, grooming, stalking and abuse. They also need to learn how to avoid the risk of exposing themselves to subsequent embarrassment.

3. ROLE OF OUR TECHNICAL STAFF

With the explosion in technology, we recognise that blocking and barring sites is no longer adequate. We need to teach all of our pupils to understand why they need to behave responsibly if they are to protect themselves. This aspect is a role for our Designated Safeguarding Lead and all our staff. Our technical staff have a key role in maintaining a safe technical infrastructure at the school and in keeping abreast with the rapid succession of technical developments. They are responsible for the security of our hardware system, our data and for training our teaching and administrative staff in the use of ICT. They monitor the use of the internet and emails and will report inappropriate usage to the Deputy Head Pastoral and Heads of Section.

4. ROLE OF OUR DESIGNATED SAFEGUARDING LEAD

We recognise that internet safety is a child protection and general safeguarding issue. The Deputy Head Pastoral, who is the Designated Safeguarding Lead (DSL), has been trained in the safety issues involved with the misuse of the internet and other mobile electronic devices. They work to promote a culture of responsible use of technology across the school community in line with national recommendations and current best practice. All of the staff with pastoral responsibilities have also received training in E-Safety issues. The school's programme on E-Safety is the Deputy Head Pastoral's responsibility, in conjunction with the Heads of Computing and PSHEE.

They will ensure that all year groups in the school are educated in the risks and the reasons why they need to behave responsibly online. It is the Deputy Head Pastoral's responsibility to handle allegations of misuse of the internet.

5. MISUSE: STATEMENT OF POLICY

We will not tolerate any illegal material, and will always report illegal activity to MASH and the police. If we discover that a child or young person is at risk as a consequence of online activity, we may seek assistance from the Child Exploitation and Online Protection Unit (CEOP). We will impose a range of sanctions on any pupil who misuses technology to bully, harass or abuse another pupil in line with our anti-bullying policy.

6. INVOLVEMENT WITH PARENTS AND GUARDIANS

We seek to work closely with parents and guardians in promoting a culture of E-Safety. We will always contact parents if we have any worries about their child's behaviour in this area, and we hope that they will feel able to share any worries with us. We recognise that not all parents and guardians may feel equipped to protect their son or daughter when they use electronic equipment at home. We therefore aim to continue to arrange sessions approximately once every two years when an outside specialist advises parents about the potential hazards of this technology, and the practical steps that parents can take to minimise the potential dangers to their children without curbing their natural enthusiasm and curiosity. In addition, we regularly communicate with parents regarding guidance on technology safety, guidelines for use of Apps on home devices and information about GSuite accounts. Pupils and parents are asked to sign a statement about responsible use of ICT at school.

7. AGREEMENT BETWEEN PUPILS, PARENTS AND THE SCHOOL FOR THE SAFE USE OF THE INTERNET AND ELECTRONIC DEVICES AT THE MANOR PREPARATORY SCHOOL

"Children and young people need to be empowered to keep themselves safe. This isn't just about a top-down approach. Children will be children - pushing boundaries and taking risks. At a public swimming pool we have gates, put up signs, have lifeguards and shallow ends; but we also teach children how to swim." Dr Tanya Byron "Safer Children in a digital world: the report of the Byron Review".

E-Safety is a whole school responsibility, and at The Manor Preparatory School, the staff and pupils have an agreement for the safe use of the internet inside the school.

- Parents of existing pupils moving up from Reception to Year 1 sign an electronic agreement at the beginning of the Autumn Term of Year 1, which is communicated via the weekly mailing
- Parents of new pupils joining Year 1 and Year 2 sign an electronic agreement on entry
- Current pupils moving up from Year 2 to Year 3 sign an agreement in their first ICT lesson at the beginning of the Autumn Term of Year 3
- New pupils joining Year 3-6 at any time are asked to sign an agreement in their first ICT lesson

The underlying principles are as follows:

a. Treating other users with respect

- We expect pupils to treat staff and each other online with the same standards of consideration and good manners as they would in the course of face to face contact. They should always follow the school's Rules and Regulations, copies of which are available on the website.
- We expect a degree of formality in communications between staff and pupils, and would not expect them to communicate with each other by text or mobile phones.
- Everyone has a right to feel secure and to be treated with respect, particularly the vulnerable. Harassment and bullying will not be tolerated. Our Anti-bullying policy is set out on the website. The school is strongly committed to promoting equal opportunities for all, regardless of race, gender, sexual orientation, physical disability or SEND.
- Staff have strict guidelines with regards to use of mobile. The mobile phones of Pre-Nursery and Nursery staff are kept in the Pre-Nursery and Nursery offices.
- All pupils are encouraged to look after each other, and to report any concerns about the misuse of technology, or worrying issue to a member of the pastoral staff.
- Pupils are not allowed mobile phones in school, unless they travel on the school buses in which case they must hand them into the school office during the day.

b. Keeping the School Network Safe

- The IT Department monitors email traffic and blocks SPAM and certain attachments.
- Access to school computers is via personal LOGIN, which is password protected. We give guidance on the reasons for always logging off and for keeping all passwords securely.
- We have strong anti-virus protection on our network, which is operated by the IT Department.
- Any member of staff or pupil, who wishes to connect a removable device to the school's network, is asked to arrange in advance with the IT Department to check it for viruses.

c. Promoting Safe Use of Technology

The whole school is taught about internet safety. From Year 1 to 6, the children are taught about E-Safety every half term in line with the Rising Stars 'Switched On Online Safety' scheme. Pupils of all ages are also encouraged to make use of the excellent online resources that are available from sites such as:

- Childnet International (www.childnet.com)
- Digizen (www.digizen.org.uk) -
- Childline Online Safety (https://www.childline.org.uk/info-advice/bullying-abuse-safety/online-mobile-safety/staying-safe-online/)
- Bullying UK (www.bullying.co.uk)

- NSPCC (www.nspcc.org.uk)

At an appropriate age, the children learn about different hazards on the internet, such as grooming, stalking, abuse, bullying, harassment and identity theft as well as the risks associated with posting blogs or photographs to the internet since they will remain in an archive even after deletion.

d. Safe Use of Personal Electronic Equipment

- Our guidance is that no one should put anything onto the web that they would not say to their grandmother!
- We offer guidance on the safe use of social networking sites and Cyber-bullying in Computing and PSHEE lessons, which covers blocking and removing contacts from "buddy lists" or 'group chats'.
- Our Computing and PSHEE lessons include guidance on how pupils can identify the signs of a cyber-stalker, and what they should do if they are worried about being harassed or stalked online.
- We offer guidance on keeping names, addresses, passwords, mobile phone numbers and other personal details safe. Privacy is essential when using the internet .
- We give guidance on how to keep safe at home

e. Considerate Use of Electronic Equipment

- Pupils' mobile phones should be switched off and stored securely in the school office during the school day. (Only pupils travelling by the Joint Bus Service can bring mobile phones to school. Mobile phones are not allowed on school trips).
- Any children who travel on the Joint Bus Service in the morning but stay in the school for a club or Extended Day must collect their phone and any other electronic device from the front office at the end of the school day as normal and hand it in to the club taker or a member of staff at Extended Day as soon as they arrive for safe-keeping until they are collected to go home. As children from Early Years attend Extended Day it is essential that this procedure is strictly adhered to.
- Sanctions may be imposed on pupils who bring any inappropriate electronic equipment into school.

SECTION B – Online Safety

Children are using technology at an ever-younger age, and so their E-Safety education should start as soon as technologies are introduced. Teachers are bound by a wider duty of care to raise awareness of E-Safety issues among children. However, the development of effective E-Safety strategies should involve all stakeholders in a child's education – staff, parents and children themselves are all integral to the process. These strategies are closely linked to other school policies such as Safeguarding, PSHEE, Anti-bullying and Cyber-bullying.

In order to ensure that we safeguard children from 'potentially harmful and inappropriate online material' (KCSIE 2019) and provide them with a safe learning environment, we implement the following:

1. How we teach online safety to children

As children begin to discover the online world and all that it can offer, so must they learn to be aware of the issues and risks, and be taught strategies for dealing with them. E-Safety must become 'second nature' to children, so that they can become safe and responsible users of technologies.

At The Manor, web-based resources are increasingly being used across the curriculum. It makes sense, therefore, that E-Safety guidance should be given to pupils wherever and whenever such use occurs, in a manner appropriate to the age, understanding and skill level of the children:

- **Teaching**

E-Safety is embedded in EYFS, Key Stages 1 and 2 Computing and PSHEE lessons, and also in other curriculum lessons where computers are used. We use a variety of selected videos and resources to educate children about the appropriate use of ICT and new technologies in and beyond school. As a guideline, we follow the Rising Stars 'Switched On Online Safety' scheme. This provides a progressive curriculum from Years 1 - 6 which we teach once every half term.

As well as showing the children how to keep themselves safe online with regards to the three main risks (content, contact, conduct), we teach the children in all lessons to be critically aware of the material they are likely to access online and guide them to validate the accuracy of information. They are also taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

- **Raising awareness on E-Safety**

Children are constantly reminded of the SMART rules (Safe, Meeting, Accepting, Reliable, Tell) with posters in every room of the school and frequent reminders by teachers. Other E-Safety displays also tell children about rules for use of ICT/Internet and raise awareness about age restrictions for social networks and how to deal with Cyber-bullying.

- **A planned programme of assemblies and workshops**

Key E-Safety messages are reinforced through dedicated workshops and national days which focus on online safety:

➢ **Childnet** representatives come to school to run online safety sessions for our whole school community: children, parents and staff. The sessions cover the benefits, and many positives, of internet use and address the related issues that children and young people face by providing practical advice. Issues covered include personal information, social networking, downloading, online grooming, sexting, Cyber-bullying, gaming, digital footprints, online reputation, and more. Childnet helps pupils become more confident in knowing what to do if something worries or upsets them online

➢ **Anti-bullying week** . The week includes a whole-school assembly followed by age-appropriate sessions (EYFS, Y1-2, Y3-4, and Y5-6) in PSHEE, form times and circle times throughout the week.

➢ The school takes part in '**Safer Internet Day**' which aims to promote the safe and responsible use of technology for young people. This takes place in February each year.

- A contract highlighting the acceptable use of technology is signed by parents and children.

2. How we help educate parents about online safety

> *'Whole-school community engagement is paramount in ensuring that the safe use of technology is communicated to all.'* (Ofsted)

Providing children at an early age with the knowledge to safeguard themselves and their personal information is crucial. But education about online safety does not stop in the classroom. With the right support, there are plenty of ways parents can be involved in the process too. In order to empower parents and help them keep their children safe online outside of school, we provide the following advice and guidance:

- **On-site training sessions about E-Safety designed especially for parents**

We invite **Childnet** and **SWSfL** to run parents' sessions at school and our Deputy Head Pastoral and Head of Computing also deliver information evenings to parents. To encourage more parents to attend our sessions about online safety, we vary the start times: Childnet will do a 9am coffee morning start time, whilst SWGfL will provide a twilight session.

A Childnet survey has found out that '*97% of parents are now feeling more confident about online safety after the training'.*

Like many schools in the country, The Manor celebrates Safer Internet Day. By dedicating a week's focus to internet safety, parents are more aware of the importance of online safety, especially when this follows a parents' training session. For Safer Internet Day, a resource pack to engage parents is provided. Anti-bullying week also raises awareness about Cyber-bullying and creates an additional focus on this issue during that week.

- **Frequent reminders on our school website**

The Manor has a dedicated section in the Parents' area of the school website, which gives carefully selected websites and guidance on online safety. These remind parents how to set the right filters in their homes and offer useful tips, such as:

What do I need to know?
Parental controls offered by your home internet provider
Parents' guide to technology
Safety tools on social networks and other online services
Supporting young people online (leaflet)
Young people and social networking sites (leaflet)
Bringing up a child in the 21st century (PowerPoint)

3. How we train the staff about online safety

Teachers are the main channel for delivering our dedicated E-Safety education in PSHEE, Computing and other curriculum lessons where technologies are being used by children. They have a duty of care to the pupils they teach and are legally responsible for all aspects of their pupils' safety, including online safety, whilst in school. Any activity involving internet use needs to be carefully planned and assessed for risk to minimise the possibility of an E-Safety incident. At The Manor, we implement the following:

- It is essential that all staff receive E-Safety training. Training is offered as follows:

  - ➢ A planned programme of formal E-Safety training is organised by the school (Childnet)

  - ➢ All new staff receive E-Safety training as part of their induction programme, ensuring that they fully understand the school E-Safety policy and Acceptable Use Policies.

  - ➢ INSET days and Twilight evening INSET sessions are used to update staff's knowledge about E-Safety.

- Teachers are likely to be the first point of contact should E-Safety incidents occur and therefore they need to be vigilant at all times and, whenever possible, identify and monitor pupils which may be at risk. Teachers can use our list of Vulnerable Children in the school to support them in doing this. Teachers are often best placed to identify changes in behaviour or family circumstances and these may indicate that a particular child is at risk from E-

Safety issues. Staff must report immediately any E-Safety concerns to the Designated Safeguarding Lead so that appropriate action can be taken early.

- Staff must themselves act as role models in the digital world and maintain a professional level of conduct in their personal use of technology, both within and outside school.

4. **Infrastructure, filtering and monitoring** (Please see Appendix 1)

SECTION C – Cyber-bullying

Please also see the school's Anti-bullying Policy

Definition of Cyber-bullying

This is defined as the use of internet (for example, emails, social websites) and/or mobile phones (for example prank calls, text messages, photographs and images) and/or other technologies which result in hurting someone's feelings.
Mr Bill Belsey, the creator of the web site: www.Cyber-bullying.org , defined this unpleasant and particularly intrusive phenomenon in the following terms:

> "Cyber-bullying involves the use of information and communication technologies to support deliberate, repeated and hostile behaviour by an individual or group that is intended to harm others."

Cyber-bullying can involve Social Networking Sites, emails and any device with an internet connection such as mobile phones used for SMS messages and as cameras.

The Manor puts the highest priority on pupils' online safety, through this Cyber-bullying Policy, the Anti-Bullying Policy and as part of Safeguarding arrangements.

a. Roles and responsibilities for online safety and the link to the school's safeguarding policy

The responsibility for online safety within the school ultimately lies with the Deputy Head Pastoral, who oversees and ensures that all aspects of the Safeguarding policy are being addressed. There are several other members of staff who also play important roles in embedding online safety within the school:

- the Computing Subject Leaders ensure online safety holds a high profile in the teaching of Computing, as well as providing pupils, parents and staff with information relating to online safety. This may involve inviting outside agencies, such as Childnet International, to the school to offer advice.
- the PSHEE Subject Leaders ensure online safety and issues such as Cyber-bullying are addressed in the PSHEE curriculum.
- the school's IT and Network Manager is responsible for ensuring firewalls are enabled to filter internet usage and monitor pupils' internet use.

b. The use of technology in the classroom and beyond for all users; permissions/restrictions and sanctions

Please also see the school's E-Safety and Acceptable Use Policy for pupils in relation to computing, mobile phones and electronic devices. Information on our technical infrastructure and how this filters and monitors inappropriate content can also be found in Section B (4) of this policy.

Staff monitor pupils' internet use closely in the classroom and in all other areas of the school, giving them specific websites to explore and teaching them how to use a search engine safely and effectively. Pupils are given clear guidance as to what is

acceptable when using the internet, both in the classroom and beyond. Pupils are not allowed to access age-restricted websites in school.

If pupils are found to be using the internet in an unacceptable manner, the school's Behaviour and Sanctions policy will be put into action. Staff and parents are aware that issues relating to Cyber-bullying and inappropriate internet use should be reported to the Deputy Head Pastoral. If the school is made aware of any misuse of the internet, the pupils' parents will be informed and an appropriate sanction enforced. Serious misdemeanours, which include any form of Cyber-bullying, will result in suspension or even exclusion from the school. (Please see the Behaviour and Sanctions Policy.)

Mobile Phones (Pupils)

Pupils are banned from bringing mobile phones to school, although pupils on the school buses and minibuses are permitted to have them for safety reasons (for example, to warn a parent that they are delayed on their journey home). They must be handed in to the School Office during the day and collected before the return coach/minibus journey.

For information about use of cameras and mobile phones by parents and staff please see section 6 of The Manor's Safeguarding Policy.

c. Building resilience in pupils to protect themselves and their peers through education and information

The Head, Deputy Head Pastoral and Heads of Computing personally address this issue in assemblies and tell children of the importance of ensuring that any online communication is totally polite. The Computing Subject Leaders and the PSHEE Subject Leaders ensure that the issue of Cyber-bullying is regularly addressed in the curriculum lessons in Key Stages 1 & 2.

A strong emphasis in all aspects of school life is placed on promoting the 'SMART' rules for internet safety (as advised by Childnet International), and regular advice is given to pupils about what to do if they encounter any issues with Cyber-bullying or inappropriate internet use. Pupils are given fictional scenarios involving such issues and are encouraged to consider how they should act, through discussion and drama activities. They key message given to pupils is: if you encounter anything online that you find upsetting, you should tell someone.

Pupils in Key Stage 2 attend talks/training sessions delivered by Childnet International, in which they are introduced to the 'SMART' rules of internet safety. Even pupils in the Foundation Stage are introduced to the idea of online safety, by promoting the message that it is important to ask for help from an adult when using the internet.

The Manor is aware that Sexting is defined as the production and/or sharing of sexual photos and videos of and by young people who are under the age of 18. It includes nude or nearly nude images and/or sexual acts. It is also referred to as 'youth produced sexual imagery.'

All such incidents should be reported to the Designated Safeguarding Lead who will manage these in line with our Safeguarding procedures. The Designated Safeguarding lead will seek immediate advice from MASH as well as the police, if MASH advise us to contact them. The Manor educates pupils about the dangers of sexting through PSHEE and Computing lessons.

d. Staff safeguarding professional development including online safety

Staff are given regular guidance and advice relating to maintaining their own professional 'digital footprint' in order to protect both themselves and their pupils. Guidance on social networking for staff can be found in the Acceptable Use Policy (For Staff). All new teaching and office staff are given guidance on the school's policy on Camera and Mobile Phone use, and the taking, using and storing images of children. They are also made aware of the school's Acceptable Use Policy (For Staff), where clear guidance is given.

Staff training led by Childnet International representatives takes place, giving the most current advice about internet safety issues and cyber-bullying.

e. Reporting mechanisms available to users to report issues and concerns to the school

If staff encounter any inappropriate emails to their school webmail account they are to contact the school's IT and Network Manager who will ensure any further emails from that particular sender are blocked. The Network Manager will also alert all other staff members to the issue.

If a child is the victim of Cyber-bullying, or suspects someone else is, they should report this to a member of staff as soon as possible and follow the general advice given to pupils in this policy. Parents aware of Cyber-bullying or misuse of the internet by a child should inform the Deputy Head Pastoral; teachers should inform their Head of Section, who will inform the The Deputy Head Pastoral who will then investigate the matter in line with our Anti-Bullying Policy. If a teacher suspects that a child has used a mobile phone inappropriately, the teacher or another teacher has the right to examine the mobile phone and report their findings to the Head.

The School has the right to intervene in pupils' emails and websites if they are suspected of being unsuitable. If any websites or pop-ups contain illegal content, the school has the duty to inform CEOP. The school, to such an extent is reasonable, is obliged to regulate the behaviour of pupils when they are off the school site (which is particularly pertinent when regulating Cyber-bullying).

Parents and pupils sign an age-appropriate 'home-school' contract, agreeing to responsible use of the internet.

f. Informing and educating parents and carers in online safety

We advise parents in letters about the dangers of children using social media sites (the School does not allow them but parents need to monitor their children's online

activities at home) and alert them to any inappropriate websites that we feel they should be made aware of. All parents and carers of pupils of any age are invited to our regular talks on internet safety delivered by Childnet International, SWGfL and our own staff. Parents are encouraged to report any concerns regarding inappropriate internet sites or communication to both the school and to the Child Exploitation Online Protection Centre, CEOP. Direct links to this organisation and Childnet International are on the school website and letters are sent to parents drawing their attention to this. Leaflets for parents produced by Childnet International are available in the school office, giving advice on internet safety and Cyber-bullying.

g. The management of personal data in line with statutory requirements

Please see the school's Data Protection Policy.

h. Guidance on official and parental photographs in school

See Safeguarding Policy about parental photographs. Official photographs for sale to parents (e.g. official school/team photographs or Sports Day photographs taken by a recognised company) are permitted and we ensure that the companies involved all have the DBS clearance for the individual photographers used.

i. Shared Information, discussion and co-operation between teachers and parents

Please see Section B of this policy.

The wider search powers included in the Education Act 2011 give teachers stronger powers to tackle Cyber-bullying by providing a specific power to search for and, if necessary, delete inappropriate images (or files) on electronic devices, including mobile phones. Separate advice on teachers' powers to search (including statutory guidance on dealing with electronic devices) is available from Childnet International.

APPENDIX 1

Firewall and Content Filtering

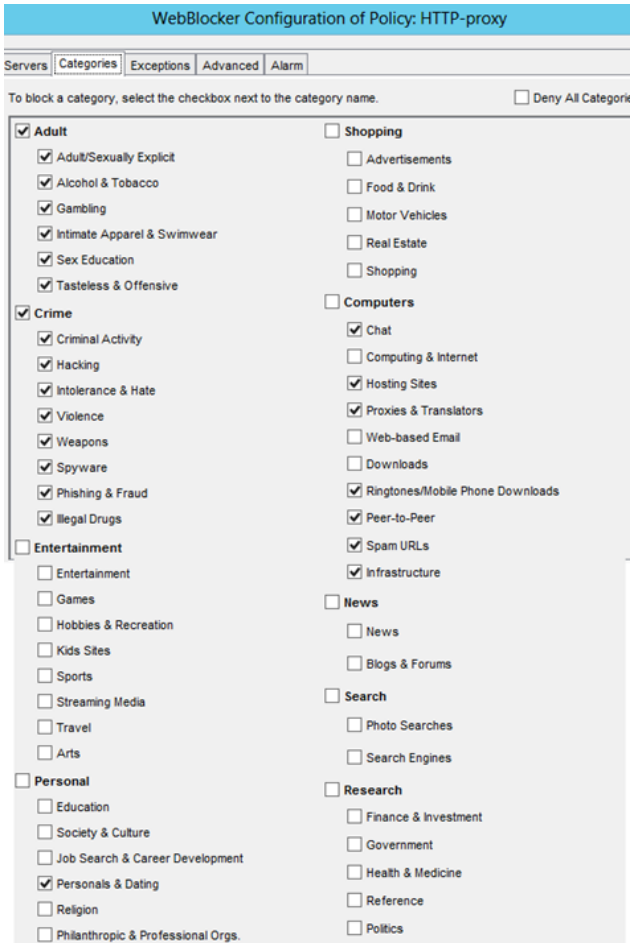
APPENDIX 1 - FIREWALL AND CONTENT FILTERING

Firewall and Content Filtering – Sophos XG

- School is using Sophos XG which is the front line defence and protects from any external threats. So any unauthorised access will not only get rejected but also get logged on the firewall logs.

- Sophos XG has a content filtering service in place which enables the school to filter inappropriate websites etc. (web/content filtering)

Sophos XG is a hardware based firewall and is used to prevent unauthorised external access to the network. Sophos XG comes with an inbuilt web and content filtering subscription service which is used to block inappropriate websites. Internet traffic can be blocked/permitted explicitly via *domain lookup*, *Host Address (IP)*, *Network Address* or *URL (web address).* The firewall uses categories to block inappropriate websites and automatically filters keywords and phrases that are pre-defined in those categories (see screen shot below). However, if a malicious website or a keyword is missed by the firewall, which is very rare, then it can be reported to the IT Manager via the ITHelpdesk@manorprep.org for this to be defined on the firewall to be blocked.



Alternatively, a site which is believed to be as inappropriate can be checked/reported to Sophos.

Content and Web filters are great tools to protect pupils from getting onto malicious websites. It blocks inappropriate content by either IP address of the website or by URL. It does not block 'keywords'. See examples below:

1) If a website www.xyz.com hosts inappropriate content it will either be blocked because it is pre-defined in a certain category on Sophos XG or it has been blocked explicitly by the Manor IT staff.

2) If someone at the Manor types in a rude phrase in Google or any other search engine, then the results would still be displayed but the actual website would get blocked.

PLEASE NOTE: The 'News' category on the firewall is not currently blocked and may display an article which is not age appropriate.

Google Safe Search

On DNS (Domain Name Server)/Network level '*Google Safe Search*' has been enforced which means that most inappropriate content will get blocked, based upon Google's decision on what is appropriate or inappropriate. This safe search cannot be disabled by the users on the network.

Youtube Filtering

At the Manor Youtube is used as an educational tool. However, Youtube is a not specifically designed for school use, due to the fact that it hosts all sorts of videos. However, in order to make things safer school has enforced '**Moderate Restricted Filter'**

Email Filtering

For Email filtering school is using Sophos Cloud Email. Unlike web content filtering Email Content Filtering works differently. Content can be blocked either by phrases and IP addresses but also keywords. There is a database of rude phrases and words that takes care of anything that is out of order.

There are cases when some legitimate emails get quarantined and have to be released manually. This can be done either by the end user or the IT Admin. Users get a daily log (via email) for Quarantined emails which they can release by clicking on the link in the received log.

IMPERO

On top of web and content filtering, School has Impero Education Pro in place. It provides a web-based interface for safeguarding staff designed to help schools to fulfil their legal duty of care around internet safety and safeguarding online. This best practice approach to safeguarding in schools, including active monitoring and logging incident captures to provide contextual insight, helps schools to identify potential risk, respond before an incident escalates, and educate students about responsible online behaviour.

Building a full picture of every learner's digital activity, Impero Education Pro's comprehensive online safety tools are designed in response to UK Government guidance and legislation including The Prevent Duty, the Department for Education's Keeping Children Safe in Education (KCSiE) guidance and the UK Safer Internet Centre's 'appropriate monitoring' provider checklist, to help schools adopt a best practice approach.

Impero Education Pro's classroom management and monitoring software empowers teaching staff with a range of classroom control, instruction and monitoring tools to help break down traditional behaviour management barriers and focus student learning. Designed to help support the requirements of UK school inspectorates, including Ofsted, ISI, Estyn and Education Scotland, the classroom management features enable teachers to facilitate technology-based teaching and learning, via one-click tools, in line with school inspectorate standards.