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

Date policy reviewed:	16 April 2020
Date of next review:	16 April 2022
Person(s) responsible for review:	SLT (VF)

CONTENTS

This policy consists of four 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 encyclopaedias 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

In order to minimise the potential for pupils to be exposed to upsetting, offensive or otherwise inappropriate material online, the following measures have been adopted. However, due to the global scale and linked nature of the internet, it is impossible to guarantee that such material will not appear on a computer screen.

- 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.

SECTION D – Acceptable Use Policy (Pupils)

The following rules cover use of all forms of IT at The Manor. All children should be aware of these rules each time they use technology at The Manor or remotely through any of our online learning platforms.

These rules are to help you to keep safe and to be respectful of others when using IT at school or when learning from home. The Manor Values also apply when you are using technology:

- Be respectful
- Be brave
- Be gentle
- Be kind and helpful
- Be conscientious and work hard
- Be a good listener
- Be honest

The Manor's Network

- The Manor's IT network should be used for school and learning purposes only
- You should only access The Manor's IT network when you have permission to do so from a member of staff
- You should only use your own username and password to log in to our network and you should keep these private (which means not sharing them with anyone)
- Only open, edit and delete your own documents and files
- Do not download or install programs or applications to the school's IT equipment
- Understand that the school monitors your use of IT equipment at all times

Using the Internet

- Use The Manor's internet for school and learning purposes only
- Use The Manor's internet only when you have permission to do so from a member of staff
- Behave in a responsible way when online. Ensure that your communications are kind, necessary and true
- Report any unpleasant or inappropriate material to a trusted adult immediately. This could be a member of staff when you are at school or somebody who looks after you at home
- Access to social networking sites is not allowed
- Never share any personal details about yourself with anyone over the internet
- Respect the copyright of digital material
- Understand that the school monitors your internet use and the sites that you visit and that your internet access is filtered at all times

Use of IT Equipment

- At The Manor, we are lucky to be able to use a range of IT equipment such as Chromebooks, iPads, computers and laptops in our lessons
- You should only use this equipment when you have permission to do so from a member of staff
- Take good care of all IT hardware at all times

- Do not eat or drink near IT equipment
- Sit comfortably when using IT equipment: adjust the chair and/or screen height if necessary
- Leave the work area clean and tidy for the next person
- Do not unplug or remove any IT equipment without the permission of a member of staff

Google Accounts

In Years 3-6, you have your own school Google account:

- Use your Google Account for school and learning purposes only
- Understand that your Google account is monitored by the school
- Only open, edit and delete your own documents and files
- Behave in a responsible way when communicating on Google Classroom, Google Drive or Google Meet. Remember that all of your communications should be kind, necessary and true
- Report unwanted or inappropriate communications to a trusted adult immediately. This could be a member of staff at school or somebody who looks after you at home

You are responsible for your behaviour and are accountable for your actions when using IT equipment, when connected to The Manor's network and when accessing the internet at home and at school. If you do not keep to these rules, sanctions, in line with our Behaviour Policy, will apply.

Remote Learning

When learning remotely, remember that all of these rules still apply to keep you safe.

Sometimes you may be taught using a video call. Remember that if you are learning from home in a video lesson with a member of staff and/or other children:

- If you are having a 1:1 lesson, you should be supervised by a parent at home
- The lesson will be recorded
- You, your teacher and anybody else in the room must wear appropriate clothing and be in an appropriate location
- We advise that pupils should not be in bedrooms for video calls but where this is not possible, the bedroom door must be open and parents must be in the vicinity
- Any language used by you, your teacher and anybody else in the room will always be appropriate and in line with our Manor Values
- Only use Google Meet if a member of staff has invited you to join the call. If there is no member of staff on the call with you, you should hang up and talk to a trusted adult at home for help
- You should not download and save any pictures or videos of your teachers. You can view these on the Google Classroom page
- Remember that if you ever feel unsure about anything that happens on a video call, you should speak to a trusted adult at home or at school so that we can help

SECTION E – Acceptable Use Policy (Staff and Visitors)

Scope of this Policy

This policy applies to all members of staff and visitors. In this policy 'staff' includes teaching and non-teaching staff, Governors and regular volunteers (but access to systems is not intended in any way to imply an employment relationship). 'Visitors' includes anyone else who comes to the school, including occasional volunteers.

Guidance for pupils can be found in in Section D (above).

Online behaviour

As a member of the school community you should follow these principles in all of your online activities, including your use of Google Classroom, Google Drive and j2e to set activities, mark work and interact with children:

- Ensure that your online communications, and any content you share online, are respectful of others and composed in a way you would wish to stand by.
- When communicating with students about their learning using Google Classroom, Google Drive and j2e, the Behaviour Policy, Anti-Bullying Policy, Cyber-Bullying Policy, Staff Behaviour Policy (found within the Safeguarding Policy) and Remote Teaching and Learning Policy should all be adhered to at all times. All of these policies can be found on the policies page of the school website here or in the 'All Policies' shared drive on Google.
- Do not access, create or share content that is illegal, deceptive, or likely to offend other members of the school community (for example, content that is obscene, or promotes violence, discrimination, or extremism, or raises safeguarding issues).
- Respect the privacy of others. Do not share photos, videos, contact details, or other information about members of the school community, even if the content is not shared publicly, without going through official channels and obtaining permission.
- Do not access or share material that infringes copyright, and do not claim the work of others as your own.
- Do not use the internet to distribute malicious software, to damage, interfere with, or gain unauthorised access to the computer systems of others, or carry out illegal activities.
- Staff should not use their personal email, or social media accounts to contact pupils or parents, and pupils and parents should not attempt to discover or contact the personal email addresses or social media accounts of staff.

Use of Social Media

While recognising the benefits social media provides, it must also be recognised that poor discipline in the use of social media can pose risks to the School, its reputation and its compliance with legal and confidentiality obligations. It is crucial that pupils,

parents and the general public have confidence in the School's decisions and standards.

This Policy aims to minimise the risks to the School of the use of social media by staff members by setting out some rules and guidelines that **ALL** staff members must adhere to. These principles are designed to ensure that staff members use social media responsibly so that the confidentiality of pupils and other staff, and the reputation of the School, are safeguarded.

This Policy does not form part of any staff member's contract of employment and the School may amend it at any time.

This Policy applies to the use of all forms of social media and all social networking sites, internet postings and blogs for School purposes, as well as for personal use that may affect the School in any way. In all cases, whether or not during business hours or term time and whether or not using the School's equipment.

a) Breaches of other policies

Social Media should never be used in a way that breaches any of the School's other policies, any laws or regulatory bodies to which you or the school is subject. If an Internet post would breach any of the School's policies in another forum, it will also breach them in an online forum.

b) General guidelines

This section provides some general guidelines for staff members using social media. They can be summarised by these two headline principles: **Use your common-sense**; and **be professional, responsible and respectful at all times.**

- When using social media, staff members must be conscious at all times of the need to keep their personal and professional lives separate. Staff members should not put themselves in a position where there is a conflict between their work for the School and their personal interests.
- Photographs, videos or any other types of image of pupils must not be uploaded onto any social media unless the consent of the pupil's family has been given.
- Staff members must not engage in activities involving social media which could damage the reputation of the School, even indirectly.
- Staff members must not represent their personal views as those of the School on any social media and should write in the first person and use a personal email address.
- Staff members must not discuss personal information about School pupils, other staff members and other professionals or ANY school information on social media.
- Staff members must not include the School's logos or other trademarks in any social media posting, or in their profiles on any social media.
- Staff members must be respectful to others when making any statement on social media and be aware that they are personally responsible for all communications which will be published on the internet for anyone to see.

- Staff members must not use social media and the internet in any way to:
    - harass, bully, unlawfully discriminate against, attack, insult, abuse, disparage or defame pupils, their family members, other staff members, other professionals, other organisations or the School as an institution;
    - make false or misleading statements; or
    - impersonate colleagues or third parties.
- Staff members must not edit open access online encyclopaedias such as Wikipedia in a personal capacity at work. This is because the source of the correction will be recorded as the School's IP address and the intervention will, therefore, appear as if it comes from the School.
- If a staff member is uncertain or concerned about the appropriateness of any statement or posting, please refrain from posting it until the matter is discussed with the Head.

c) Personal use of social media

The School permits limited personal use of social media while at work. Staff members are expected to devote their contracted hours of work to their professional duties and, in practice, personal use of the internet or social media should not be done during contact time (for teachers and teacher assistants), should never involve unprofessional or inappropriate content and must always comply with this policy. In particular with regard to personal use of social media, staff members should bear the following in mind:

- School email addresses and other official contact details must not be used for setting up personal social media accounts, or to communicate through such media. The use of School email addresses to create or join a School sanctioned social media site is appropriate.
- Staff members must not identify themselves as employees of the School, or service providers for the School, in their personal social media profiles. The content of professional social media profiles, such as those on LinkedIn, is up to the user's discretion.
- Staff members should keep in mind that anyone, such as parents, students and colleagues, could access their profile. This is to prevent information on these sites being linked with the School and to safeguard the privacy of staff members, particularly those involved in providing sensitive front line services.
- Staff members must decline 'friend requests' from current and previous pupils (up to the age of 18) that they receive in their personal social media accounts.
- Staff members must not "check in" or tag their photos/videos at the School.
- Staff members must be mindful of connecting with colleagues on social media as it may be difficult to maintain professional relationships, or it might be just embarrassing if too much personal information is known in the work place.
- Staff members must not have contact through any personal social media with:
    - any current pupils, whether from the School or any other school, unless it is for professional contact or the pupils are family members; or

- pupils' family members, if that contact is likely to constitute a conflict of interest or call into question their objectivity.

- Staff members are strongly advised to ensure that they set the privacy levels of their personal sites as strictly as they can and opt out of public listings on social networking sites to protect their own privacy.

d) Using social media on behalf of the school

Staff members can only use officially sanctioned School social media tools for communication on behalf of the School. Requests for this type of communication should go via the Head and will be always be subject to the following additional principles:

- There must be a strong pedagogical or business reason for creating official School social network profiles to communicate with pupils or others. Staff members must not create profiles for trivial reasons which could expose the School to unwelcome publicity, the posting of unwelcome material or to damage to its reputation.
- Official school profiles must be created according to the requirements provided by the Head. Profiles created must not breach the terms and conditions of social media service providers, particularly with regard to minimum age requirements.
- Staff members must be accurate, fair and transparent when creating or altering online sources of information on behalf of the School.
- If a staff member's duties include speaking on behalf of the School in a social media environment, such communications must still be approved by the Head before being published, posted or sent. Likewise, if a staff member is contacted by anyone for comments about the School, such inquiries should be directed to the Head and not responded to directly without that person's approval.

We are responsible at all times for the safeguarding and protection of the children under our care. Staff members must at all times act in the best interests of children and young people when creating, participating in or contributing content to social media sites.

e) Monitoring

The School reserves the right to monitor, intercept and review, without further notice, staff members' activities using the School's IT resources and communications systems, including but not limited to social media postings and activities, to ensure that the School's rules are being complied with and for legitimate School purposes, and staff members consent to such monitoring by their use of such resources and systems.

Staff members should not use the School's IT resources and communications systems for any matter that they wish to keep private or confidential from the School. The contents of the School's IT resources and communications systems are the property of the School. Staff members have no expectation of privacy in any message, file, data, document, facsimile, telephone conversation, social media post or message, or any other kind of information or data transmitted to, received or printed from, or stored on the School's equipment.

f) Communication with Pupils Online

i. Social Media

On leaving the service of the School, staff members must not contact any of the School's current pupils by means of personal social media sites. For the avoidance of doubt, this also includes previous pupils under the age of 18.

ii. Online Learning Platforms

Children have access to a variety of online learning platforms at The Manor. Some of these platforms such as Google Classroom, Google Drive and j2e provide opportunities for staff to communicate with pupils about their learning through comments and private messages.

In all staff communication with pupils on School-approved learning platforms, staff must understand that it is their duty to promote E-Safety with the children in their care, to report any matters of concern, and to use electronic communications of any kind in a professional and responsible manner:

- Staff are expected to help children to develop a responsible attitude to system use, communications and publishing when using online learning platforms
- Staff must report any incidents of concern regarding children's safety to the DSL
- Staff must ensure that electronic communications with pupils including email and instant messages are compatible with their professional role and that messages cannot be misunderstood or misinterpreted

iii. Video Lessons

When teaching remotely, staff may record videos or live-stream a lesson using video technology via our Google Meet platform. It is of paramount importance that in these cases, the following rules are followed to ensure best Safeguarding practice:

- Every lesson must be recorded and automatically saved on the school's Google database to ensure best Safeguarding practice. Teachers must click 'record' at the start of each lesson and click to end the recording before closing the browser
- Videos must never be downloaded to your device
- Staff must ensure that their device is used in an appropriate area and where possible, against a neutral background. Under no circumstances should video lessons take place in bedrooms
- Language and clothing must be professional and appropriate at all times
- No adults or children who are not members of staff or pupils at The Manor should feature in video lessons
- Children and their families will also sign an agreement to ensure their appropriate use of the technology, language, filming locations and clothing. Where a member of staff feels that these rules are not being followed, they should end the call immediately and then contact their line manager for advice
- In the case of 1:1 video lessons, parents will sign an agreement to supervise their child and if staff find that this is not the case, staff must end the call and contact their line manager for advice

- If a Safeguarding concern comes to light during interactions with the children, The Manor's Safeguarding procedures to report the concern as soon as possible must be followed

g) Recruitment and references

The School may use internet searches to perform due diligence on candidates in the course of recruitment. Where the School does this, the School will act in accordance with the School's data protection and equal opportunities obligations.

Staff members should never provide references for other individuals on social or professional networking sites. Such references, whether positive or negative, can be attributed to the School and create legal liability for both the author of the reference and the School.

h) Breaches

Heads of Section have a specific responsibility for ensuring that this Policy is adhered to, ensuring that all staff members in their department understand the standards of behaviour expected of them and taking action when behaviour falls below those standards.

All staff members are responsible for the success of this Policy and should ensure that they take the time to read and understand it. If any staff member sees social media content that disparages or reflects poorly on the School, please contact the Head.

Staff member(s) may be required to remove any social media content that the School considers to constitute a breach of this policy. Failure to comply with such a request may in itself result in disciplinary action.

Any breach of this Policy may lead to disciplinary action being taken against the staff member(s) involved up to and including dismissal, in line with the School's Disciplinary Policy for Staff. Any staff member(s) suspected of committing a breach of this Policy will be required to co-operate with the School's investigation, which may involve handing over relevant passwords and login details.

Using the school's IT systems

Whenever you use the school's IT systems and G Suite (including by connecting your own device to the network) you should follow these principles:

- Only access school IT systems and G Suite using your own username and password. Do not share your username or password with anyone else
- Do not attempt to circumvent the content filters or other security measures installed on the school's IT systems or G Suite, and do not attempt to access parts of the system that you do not have permission to access
- Do not attempt to install software on, or otherwise alter, school IT systems or G Suite
- Do not use the school's IT systems or G Suite in a way that breaches the principles of online behaviour set out above
- Remember that the school monitors use of the school's IT systems and G Suite, and that the school can view content accessed or sent via its systems

- All resources and websites used for delivering lessons on the school's IT systems and G Suite should be thoroughly checked before use. Staff must not expose children to inappropriate images or material in their use of IT systems and G Suite

Passwords

Passwords protect the School's network and computer system and are your responsibility. They should not be obvious (for example "password", 123456, a family name or birthdays), and nor should they be the same as your widely-used personal passwords. You should not let anyone else know your password, nor keep a list of passwords where they may be accessed, and must change it immediately if it appears to be compromised. You should not attempt to gain unauthorised access to anyone else's computer or to confidential information to which you do not have access rights.

Use of Property

Any property belonging to the School should be treated with respect and care, and used only in accordance with any training and policies provided. You must report any faults or breakages without delay to the IT Manager or Bursar.

Use of school systems

The provision of school email accounts, Wi-Fi and internet access is for official school business, administration and education. Staff and pupils should keep their personal, family and social lives separate from their school IT use and limit as far as possible any personal use of these accounts. Again, please be aware of the school's right to monitor and access web history and email use.

Use of personal devices or accounts and working remotely

All official school business must be conducted on school systems, and it is not permissible to use personal email accounts for school business. Any use of personal devices for school purposes, and any removal of personal data or confidential information from school systems – by any means including email, printing, file transfer, cloud or (encrypted) memory stick – must be registered and approved by the Bursar.

Where permission is given for use of personal devices, these must be subject to appropriate safeguards in line with the school's policies. Please see Bring Your Own Device Policy and Data Protection Policy.

Monitoring and access

Staff, parents and pupils should be aware that school email and internet usage (including through school Wi-Fi) will be monitored for safeguarding, conduct and performance purposes, and both web history and school email accounts may be accessed by the school where necessary for a lawful purpose – including serious conduct or welfare concerns, extremism and the protection of others.

Any personal devices used by pupils, whether or not such use is permitted, may be confiscated and examined under such circumstances. The school may require staff to conduct searches of their personal accounts or devices if they were used for school business in contravention of this policy.

Retention of digital data

Email accounts will be closed and the contents deleted on the first day of the new term after which a staff member has left. Important information that is necessary to be kept should be held on the relevant personnel or pupil file, not kept in personal folders, archives or inboxes. Hence it is the responsibility of each account user to ensure that important information (or indeed any personal information that they wish to keep, in line with school policy on personal use) is retained in the right place or, where applicable, provided to the right colleague. That way no important information should ever be lost as a result of the school's email deletion protocol.

If you consider that reasons exist for the protocol not to apply, or need assistance in how to retain and appropriately archive data, please contact the IT Manager.

Photographs

- Many school activities involve recording images as part of the curriculum, extra-curricular activities, publicity or to celebrate an achievement. In accordance with The Data Protection Act 1998, the image of a pupil is personal data. Therefore, it is a requirement under the Act for consent to be obtained from the parent/guardian of a pupil for any images made. It is also important to take into account the wishes of the pupil, remembering that some pupils do not wish to have their photograph taken or be filmed
- Personal mobile phones and cameras which staff have on the school premises should not be used to take photographs of the children
- Only school mobile phones and cameras should be used for taking photographs and then images or videos should only be downloaded onto school computers, so that their use can be monitored
- All photographs/stills and video footage should be available for scrutiny and staff should be able to justify all images/video footage made
- Mobile phones are not permitted in the EYFS setting
- Images and videos of children at The Manor should never be stored on personal devices
- Staff should remain aware of the potential for images of pupils to be misused to create indecent images of children and/or for grooming purposes. Therefore, careful consideration should be given to how activities which are being filmed or photographed are organised and undertaken. Particular care should be given when filming or photographing young or vulnerable pupils who may be unable to question how or why the activities are taking place. Staff should also be mindful that pupils who have been abused through the use of video or photography may feel threatened by its use in a teaching environment.

Breaches of this policy

A deliberate breach of this policy will be dealt with as a disciplinary matter using the school's usual procedures. In addition, a deliberate breach may result in the school restricting your access to school IT systems.

If you become aware of a breach of this policy or the E-Safety Policy, or you are concerned that a member of the school community is being harassed or harmed online you should report it to the Head. Reports will be treated in confidence.

SECTION F – Remote Learning

Please also see the Remote Teaching and Learning Policy.

Use of Electronic Equipment for Remote Learning during School Closure
In the case of school closure, the following precautions apply for the use of technology for remote learning in Years 3 - 6:

1. Temporary Loan of School Chromebooks

1.1 Ownership of Chromebooks
In the event of school closure, School Chromebooks may be loaned to children to access their learning remotely via Google Drive.

For the purposes of this scheme, ownership of the Chromebooks is defined as 'school-owned' (they have been purchased directly by The Manor).

1.2 Distribution of Chromebooks
Chromebooks will be distributed from the Main Office. Prior to collecting these Chromebooks, all parents must sign a Home-School agreement for the safe and appropriate use of these devices at home (see appendix).

2. Taking care of Chromebooks

Students and parents are responsible for the general care of the school-owned Chromebook they have been issued with by The Manor. School-owned Chromebooks that are broken or fail to work properly must be returned to The Manor, if safe to do so, for an evaluation of the equipment / repair / replacement.

2.1 General Precautions
All remote Chromebook users will follow this E-Safety and Acceptable Use Policy.

- Only use a clean, soft cloth to clean the screen, no cleansers of any type
- Cables must be inserted carefully into the Chromebook to prevent damage
- Chromebooks themselves must remain free of any writing, drawing, stickers, or labels that are not the property of The Manor.
- Chromebooks must never be left in an unlocked locker, unlocked car or any unsupervised area.
- Students and parents are responsible for keeping their Chromebook's battery charged for use during the day to access learning.

2.2 Carrying Chromebooks
When carrying Chromebooks the following guidelines should be followed:

- Chromebooks should always be closed when being carried
- Some bags / rucksacks hold other objects; these must be kept to a minimum to avoid placing too much pressure and weight on the Chromebook screen if the Chromebook is to be carried in this way.

2.3 Screen care
The Chromebook screens can be damaged if subjected to rough treatment.

- Do not lean on top of the Chromebook when it is closed
- Do not place anything near or on top of the Chromebook that could put pressure on the screen
- Clean the screen with a soft, dry cloth or anti-static cloth
- Do not “bump” the Chromebook against lockers, walls, car doors, floors, etc. as it could potentially break the screen.

3. Home internet access

Students are allowed to connect to home wireless networks on their Chromebooks so that they can be used as a learning device. The Chromebooks should not be connected to other devices at home such as printers. If needed, advice is available from The Manor’s IT Manager. The Manor does not take any responsibility for providing any out of school access to the internet or printing facilities.

4. Managing files and saving work

Students are taught how to save their work to the appropriate locations on Google Drive using their personal login information. It is expected that all work will be saved on the children’s Google Drive or Google Classroom pages and shared with staff via the ‘share’ feature on these platforms. It is the student’s responsibility to ensure that work is not lost due to accidental deletion although this can be recovered by The Manor staff.

5. Software on Chromebooks

5.1 Originally installed software

The software originally installed by The Manor must remain on the Chromebook in usable condition and be easily accessible at all times. From time to time the school may add software applications to the Chromebook although this will not take place remotely.

5.2 Software upgrades

Upgrade versions of licensed software are available from time to time and these will be installed on site at The Manor when Chromebooks are returned to school after closure.

6. Acceptable Use

The use of The Manor’s technology resources is a privilege. The privilege of using the technology resources provided by The Manor is not transferable or extendable to students or other people / groups outside the school and terminates when a student is no longer enrolled at The Manor. This policy is provided to make all users aware of the responsibilities associated with efficient, ethical and lawful use of technology resources. If a person violates any User Terms and Conditions named in this policy, privileges may be terminated, access to the technology resources may be denied, and appropriate disciplinary action shall be applied.

Violations may result in sanctions in line with our Behaviour Policy.

6.1 School responsibilities during periods of remote learning:

- Provide the opportunity for Year 3 - 6 children to be given Chromebooks on a temporary basis during closure.
- Provide access to Google Drive and associated Google applications to its students
- Provide guidance to aid students and parents in using the devices in their learning and help assure compliance with the acceptable use policy.

The Manor reserves the right to review, monitor and restrict information stored on or transmitted via The Manor school-owned equipment and to investigate inappropriate use of resources which includes monitoring of Google Drive and associated Google applications; subject to the correct protocol being applied.

6.2 Students are responsible for:

- Using Chromebooks / devices in a responsible and ethical manner
- Obeying general school rules concerning behaviour and communication when working on Chromebooks or computers
- Using all technology resources in an appropriate manner in order to avoid damage to school equipment or the school's network systems.
- Speaking to their parents about any security problems that they may encounter so that the IT Manager can be contacted.
- Turning off their Chromebook after they have finished working to protect their work and information.

6.3 Parents are responsible for:

- Helping The Manor protect our computer systems /devices by contacting the IT Manager about any security problems they may encounter.
- Monitoring activity on their child's account
- Returning the Chromebook to The Manor at the end of the loan period. Students who withdraw, are suspended or excluded, or leave The Manor for any other reason before the end of the loan period must return their Chromebook to The Manor on or before the date of leaving.

Use of any information obtained via The Manor's Google Drive platform or associated platforms is at your own risk. The Manor specifically denies any responsibility for the accuracy or quality for information provided by third parties which has been obtained through its services.

6.4 Student activities strictly prohibited:

- Illegal installation or transmission of copyrighted materials.
- Any action that violates existing Exam Board policy or public law.
- Sending, accessing, uploading, downloading or distributing offensive, profane, threatening, pornographic, obscene, or sexually explicit materials.
- Use of sites selling exam papers, book reports and other forms of student work.
- Changing of Chromebook settings (exceptions include personal settings such as font size, brightness, etc.) that would stop the device working as it was originally set up and intended to work.
- Spamming - sending mass or inappropriate messages via their Google account.
- Gaining access to other users' accounts, files, and / or data.

- Use of the school's internet/e-mail accounts for financial or commercial gain or for any illegal activity.
- Participation in credit card fraud, electronic forgery or other forms of illegal behaviour.
- Vandalism (any malicious attempt to harm or destroy hardware, software or data, including, but not limited to, the uploading or creation of computer viruses or computer programs that can infiltrate computer systems and/or damage software components) of school equipment will not be allowed.
- Transmission or accessing materials that are obscene, pornographic, offensive, threatening or otherwise intended to harass or demean recipients.

6.5. Legal propriety:

- Students must comply with trademark and copyright laws and all license agreements. Ignorance of the law does NOT guarantee immunity from prosecution. If you are unsure, ask a teacher or parent / carer.
- Plagiarism is a violation of The Manor ethos. Students must give credit to all sources used, whether quoted or summarised. This includes all forms of media on the Internet, such as graphics, movies, music and text. Exam Boards, if notified, would most probably remove any entry to an exam / disqualify a student / remove qualification.
- Use or possession of hacking software is strictly prohibited and violators will be subject to investigation and punishment by the School and could be reported to the police.

6.6 Student Discipline

If a student is deemed to break any of the conditions as set out in this policy, they will be issued with a warning. They will have a meeting with an appropriate member of staff to discuss the implications of their actions. The school will inform parents of the issue causing concern. If the student breaks a rule for a second time, the school will follow our Behaviour Policy for appropriate sanctions and this may include confiscation of the Chromebook if this has been agreed with parents.

7. Chromebook Identification

Student Chromebooks will be labelled in the manner specified by the school. Chromebooks can be identified in the following ways:

Student Chromebooks will be labelled in the manner specified by the school. Chromebooks can be identified in the following ways:

- Record of serial number
- The Manor Fixed Asset Number

8. **Repair and Replacement of Chromebooks**

8.1 Protection for Family-owned Devices

Insuring or covering of Chromebooks during the loan period is the responsibility of parents.

8.2 Repairs to School-owned Devices

Students will be held responsible for all damage to their Chromebooks including, but not limited to: broken screens, cracked plastic pieces, inoperability, etc. **where this**

damage has been caused deliberately or through neglect. Should the cost to repair exceed the cost of purchasing a new device, parents will pay for full replacement value. Lost items such as cases and loaned cables will be charged at the actual full replacement cost. Students or parents should report any damage to the IT Manger as soon as it occurs.

9. The Manor Chromebook Home-School Agreement

Please see Appendix 2.

APPENDIX 1

Firewall and Content Filtering

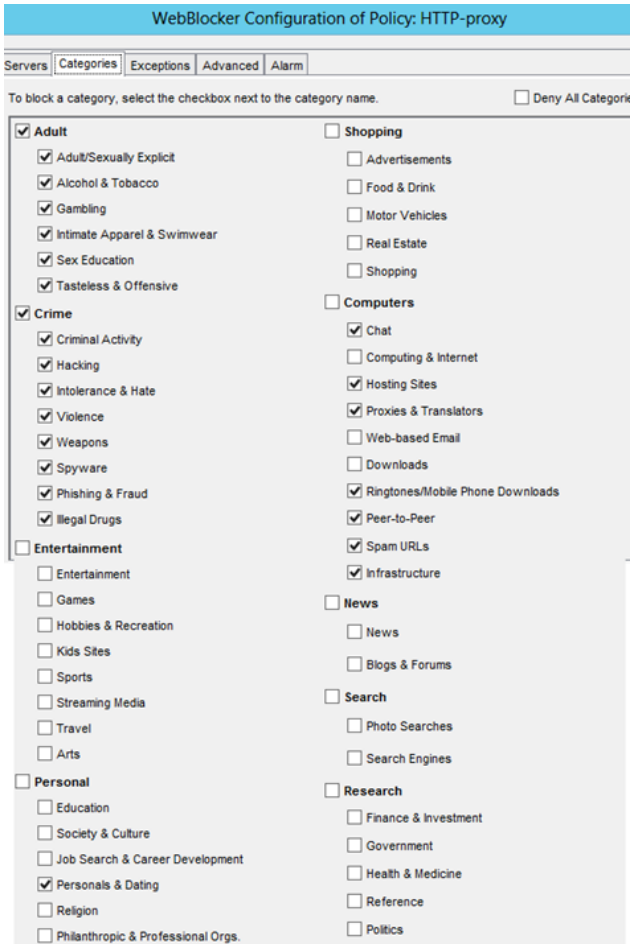
APPENDIX 1 - FIREWALL AND CONTENT FILTERING

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.

APPENDIX 2

THE MANOR CHROMEBOOK HOME SCHOOL AGREEMENT - MARCH 2020

We are sending home individual Chromebooks with your child as a helpful way for them to access their learning during school closure.

We also want to ensure that our pupils are responsible and considerate users of technology and provide a safe and structured environment in which to develop these attributes. This Home School Agreement sets out the terms for the use of school-provided Chromebooks in March 2020.

SECTION A: Pupil Code of Conduct:

1. The Chromebook you have been assigned is your responsibility.
2. Your Chromebook may be used for academic work only and you must ask permission from the person who looks after you before using it.
3. Your parents have the right to access your Chromebook at any time and school will be able to view your screen at any time.
4. Inappropriate use of your Chromebook will result in sanctions from the school's behaviour policy.
5. Pupils must agree to this agreement.

SECTION B: Pupil Agreement

As a pupil I agree to:

1. Look after my Chromebook carefully.
2. Immediately let my parents know if the Chromebook is lost or damaged.
3. Not delete the search history in my Internet browser or enable "Private" browsing.
4. Tell the person who looks after me at once if I see web pages or emails that are offensive or worry me.
5. Not use my Chromebook to share copyrighted material.
6. Only access the school network and Internet using my own school username and password, and not access files belonging to others.
7. Use the camera (photo or video) for school purposes only if a member of staff has asked me to for an activity.
8. Never access inappropriate content on my Chromebook.
9. Not remove any stickers which identify my Chromebook.
10. When using the Internet and sending emails I will protect myself and others by not giving out personal information.
11. Ensure that any emails or communications are polite, sensible and responsible.
12. Not allow anybody else to borrow my Chromebook.

SECTION C: Parent/ Guardian Agreement

As a parent/ guardian I agree to:

1. Ensure that my child looks after their school Chromebook appropriately.
2. Configure the WiFi/ internet in the home environment such that the Chromebook is able to connect and that only appropriate content/ websites are accessed on their school Chromebook.

3. Monitor my child's use of the internet at home, and to ensure that only appropriate content/ websites are accessed on their school Chromebook using the WiFi/ internet connection in the home environment.
4. Check the contents of my child's Chromebook weekly (e.g. photos, browsing history).
5. Provide the school with feedback about your child's Chromebook and their usage as requested.
6. In the first occurrence of damage to the Chromebook that is not covered by any warranty agreement the Chromebook may be under, to contribute to the replacement cost (see table below for pricing). Such damage includes, but is not limited to, cracked screens and accidental damage.
7. In any subsequent occurrence of damage to the Chromebook that is not covered by any warranty agreement the Chromebook may be under, to cover the full replacement cost (see table below for pricing). Such damage includes, but is not limited to, cracked screens and accidental damage.
8. Cover the cost of a new Chromebook in the event of it being lost or stolen (see table below for pricing)
9. Return Chromebook and charger in working order. All items that are not returned in working order will be replaced by the school and the cost will be added to your school bill.

Note: You may wish to consider adding the Chromebook to your home insurance, in which case we are able to provide details for you in the event of a claim.

SECTION D: School Agreement

The School agrees to:

1. Provide a Chromebook to pupils in Years 3 to 6 who have requested one.
2. Provide infrastructure for the effective use of Chromebooks at home (via Google Drive).
3. Ensure that students are familiar with how to log into Chromebooks and use them to access Google Drive and Google Classroom resources.
4. Provide parents and guardians with ongoing advice to help them support their child's use of their Chromebook.

Note: The school will not be responsible for any content accessed when the internet is used outside of the school site.

TERMS AND CONDITIONS

1. Failure to take reasonable care or to abide by the other conditions listed in this document and any applicable policies will result in sanctions according to the school behaviour policy.
2. The school will not be responsible for any outcomes which may occur if guidelines are not followed.
3. The school cannot accept responsibility for the electrical costs involved in charging Chromebooks at home.
4. The Chromebook (and hardware, software, services and applications provided by the school) will remain the property of the school.

Item	Price
Replacement Chromebook (first replacement)	£175
Replacement Chromebook and charger (second and subsequent replacement)	£350

The following policies, which can be found on the school website, apply to the use and handling of the Chromebook:

- E-Safety and Acceptable Use Policy
- Cyber-bullying Policy
- Data Protection Policy

Pupil name:	
Parent name:	
Parent signature:	
Date:	

FOR OFFICE USE ONLY - Individual Chromebook Fixed Asset Number: