The Manor
Preparatory School

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

Date policy reviewed:	1 September 2024
Date of next review:	1 September 2025
Person(s) responsible for review:	SLT (VF)

CONTENTS

This policy is includes the following sections:

SECTION A - General Overview, including Safeguarding

1. TECHNOLOGY IN THE CURRICULUM

Technology is a crucial component of every academic subject, and is also taught as a subject in its own right. Our classrooms are equipped with interactive whiteboards and in addition to our ICT suites, we have a number of Chromebooks, laptops and iPads available for use by the pupils. Children in Years 3 to 6 have an individual Chromebook loaned to them to support them in their learning. 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, extremist 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

It is recognised by The Manor Preparatory School that the use of technology presents challenges and risks to children and adults both inside and outside of school.

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 be aware of their digital footprint and how to behave responsibly online.

3. ROLE OF OUR TECHNICAL STAFF

Our technical staff and contractors 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 work with the Deputy Head Pastoral (as Designated Safeguarding Lead) to monitor the use of the internet and emails, as well as maintaining effective filtering and monitoring systems, and reporting on these areas to the Head and the Governing Board. We recognise that in addition to blocking and barring online content, 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 led by our Designated Safeguarding Lead, supported by the Head of Computing and Pre-Prep Computing Coordinator, and is a responsibility of all our staff.

4. SAFEGUARDING AND THE ROLE OF OUR DESIGNATED SAFEGUARDING LEAD

It is essential that children are safeguarded from potentially harmful and inappropriate online material. The Manor is fully aware of the importance of an effective whole school approach to online safety, to empower us to protect and educate pupils, staff and parents in their use of technology, and establishes mechanisms to identify, intervene and escalate any incident where appropriate. Online safety is a running and interrelated theme when devising and implementing policies and procedures. Online safety is also considered whilst planning the curriculum, any teacher training, the role and responsibilities of the Designated Safeguarding Lead and any parental engagement.

The Deputy Head Pastoral, who is the Designated Safeguarding Lead (DSL), has overall responsibility for online safety at The Manor, supported by the Head of Computing and Pre-Prep Computing Coordinator, and 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. The school's curriculum on E-Safety is led and overseen by the Deputy Head Pastoral, Head of Computing, Pre-Prep Computing Coordinator and Head of Learning for Life (PSHEE/PSED). They will ensure that all year groups in the school are educated about online risks and responsible online behaviour. It is the Deputy Head Pastoral's responsibility to handle allegations of misuse of the internet or issues which arise in relation to our filtering and monitoring systems.

The Head, DSL, Deputy DSLs, the leadership team and all staff are aware of the online safety advice contained within 'Keeping Children Safe in Education 2024'.

All of the staff with pastoral and teaching responsibilities have also received training in E-Safety issues.

The Manor regularly assesses online safety risks and reviews our approach using the LgFL Online Safety Audit and Risk Assessment form, as recommended in 'Keeping Children Safe in Education 2024'.

5. RADICALISATION AND EXTREMISM

As part of the Prevent agenda, The Manor will ensure an effective filtering and monitoring system to prevent radicalisation and access to extremist views, as well as teaching children how to stay safe online and who to speak to if they have any concerns or receive any inappropriate communication online.

Staff are made aware at Safeguarding training of the characteristics within children and families that may indicate radicalisation or warning indicators of those who may be vulnerable to radicalisation. Staff also have training to ensure they understand our expectations, applicable roles and responsibilities in relation to filtering and monitoring.

The Manor’s Safeguarding Policy covers further detail of the Prevent Duty and how this is implemented at The Manor.

Reporting concerns regarding radicalisation and extremism:

Staff will respond to any radicalisation/extremism concerns in the same manner as Safeguarding concerns and will follow The Manor’s Safeguarding Policy and procedures.

As part of the pupil Acceptable Use Policy, it outlines that children must only use the school systems for learning and that if they see any inappropriate material, they should report this to a member of staff.

6. MISUSE: STATEMENT OF POLICY

We will not tolerate any illegal material, and will always report illegal activity to MASH and/or the police. If we discover that a child or young person is at risk as a consequence of online activity, we may also 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 and Behaviour, Discipline and Exclusion Policy. Bullying on the basis of protected characteristics is taken particularly seriously and The Manor distinguishes incidents of this type of bullying in our records.

7. 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 concerns about their child’s online activity, and we encourage them to share any concerns with us. We recognise that not all parents and guardians may feel equipped to protect their child 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 online safety, guidelines for use of apps on home devices and information about Google accounts. This includes through newsletters, emails and parent talks.

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

E-Safety is a whole school responsibility, and at The Manor Preparatory School, staff, pupils and parents are expected to adhere to the Acceptable Use Policy for the safe use of the internet and technology inside the school and when accessing learning remotely.

- Parents of new pupils joining The Manor sign an electronic agreement on entry to confirm that they have read the E-Safety and Acceptable Use Policy and discussed this with their child.
- Current pupils in Year 1-6 have a talk from their Form and/or Computing teachers at the start of each academic year, in which the Acceptable Use Policy is discussed. This message is then reinforced in formal E-Safety lessons.

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 Manor Values, a copy of which is 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, including the vulnerable. Harassment and bullying will not be tolerated, as set out in our Anti-Bullying Policy. The school is strongly committed to promoting equal opportunities for all, regardless of race, gender, sexual orientation, physical disability, SEND or any of the protected characteristics
- Staff have strict guidelines with regards to use of mobile devices; these are not to be used in the vicinity of children. For Early Years staff, phones must be kept in a designated staff area or a locked cupboard during the school day.
- All pupils are encouraged to look after each other, and to report any concerns about the misuse of technology, or worrying issues to a member of 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 for the duration of 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 technical support staff monitor email traffic and block spam and certain attachments.
- Access to school computers and Google Drive 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 our technical support staff
- 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 our technical staff to check it for viruses.
- Our Deputy Head Pastoral (as Designated Safeguarding Lead) monitors user activity online and works with our technical support staff to maintain effective

filtering and monitoring systems. This includes responding to alerts sent to the Deputy Head Pastoral whenever inappropriate content is flagged by our 'Securly' monitoring system. The Deputy Head Pastoral meets regularly with the Head and Safeguarding Governor on matters of filtering and monitoring to ensure we continually review this area. An annual review of filtering and monitoring at The Manor also takes place with the Senior Leadership Team (including the Deputy Head Pastoral), IT Service Provider, Computing leads and Safeguarding Governor in attendance.

c. Promoting Safe Use of Technology, including Personal Electronic Equipment

The whole school is taught about online safety. This helps the children to build resilience to protect themselves and their peers through education and information. 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:

- Google - Be Internet Awesome (https://beinternetawesome.withgoogle.com/en_us/interland)
- Childnet International (www.childnet.com)
- Childline Online Safety (https://www.childline.org.uk/info-advice/bullying-abuse-safety/online-mobile-safety/staying-safe-online/)
- NSPCC (www.nspcc.org.uk)
- Think U Know - CEOP Education (https://www.thinkuknow.co.uk/)
- UK Safer Internet Centre (www.saferinternet.org.uk)
- Internet matters (www.internetmatters.org)

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 online gaming, copyright, and posting blogs or photographs to the internet since they will remain in an archive even after deletion. Our lessons also teach children about keeping personal information safe, digital citizenship, playing games online, responsible internet use and developing resilience at home and at school.

We regularly remind the children of the Childnet 'Be SMART Online' rules for staying safe online in Years 3-6 and use 'Smartie the Penguin' with younger children to teach them to tell someone when they encounter something worrying online.

We offer guidance on the safe use of social networking sites and cyber-bullying in Computing and Learning for Life (PSHEE/PSED) lessons, including guidance on how pupils can identify the signs of cyber-bullying, grooming or harassment, and what they should do if they are worried about any online communication of this nature. This includes speaking to a trusted adult, blocking, saving evidence and reporting incidents.

d. Use of Mobile Technology and 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.

To mitigate the risks associated with mobile phone use, children from The Manor are sat at the front of the JBS buses, where it is easier for them to be supervised. We tell the children not to use their mobile phones when on the JBS unless they are contacting a parent, and any concerns raised by JBS staff will be passed on to the Deputy Head Pastoral, to be followed up on by The Manor.

Sanctions may be imposed on pupils who bring any inappropriate electronic equipment into school.

The Manor are aware of the DfE's guidance document: 'Mobile phones in schools - Guidance for schools on prohibiting the use of mobile phones throughout the school day' (February 2024).

SECTION B – Online Safety

Children are using technology at an ever-younger age, and so their online 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, Learning for Life (PSHEE/PSED), Anti-bullying and Cyber-bullying.

The Manor Preparatory School will ensure a comprehensive whole school curriculum response is in place to enable all pupils to learn about and manage online risks effectively and will support parents and the wider school community (including all members of staff) to become aware and alert to the need to keep children safe online.

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 used extensively 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 Learning for Life (PSHEE/PSED) 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.

In Years 1-6, we follow the Rising Stars 'Switched On Online Safety' scheme of work in Computing lessons, which provides a progressive curriculum. We teach these lessons once every half term. In Learning for Life (PSHEE/PSED), we follow the 'Jigsaw' scheme of work, addressing online safety in our 'Healthy Me', 'Relationships' and 'Changing Me' topics. Please also see our Learning for Life (PSHEE/PSED) Policy and RSHE (Relationships, Sex and Health Education) Policy.

We focus mainly on the four key areas of risk outlined in Keeping Children Safe in Education 2024:

- content: being exposed to illegal, inappropriate or harmful content; for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.

- contact: being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.

- conduct: personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying; and

- commerce: risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

In addition to this, 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.

The Manor recognises that a one size fits all approach may not be appropriate for all children, and a more personalised or contextualised approach for more vulnerable children, victims of abuse and some SEND children might be needed.

Children with SEND

We recognise that children with SEND may experience greater risk when it comes to content, contact, conduct or commerce risks.

The 'Internet Matters' advice document on 'Supporting children and young people with SEND online' details important considerations about the additional vulnerabilities of children with SEND online:

- Children and young people with SEND are more likely to experience all online risks compared to those without any difficulties, particularly contact risks
- Examples of this include sexting under pressure and coercion. They appear to be preyed upon and singled out.
- Children and young people with communication difficulties are also more likely to experience contact risks.
- Experiencing contact risks is also associated with a greater risk of seeing harmful content and experiencing more aggressive behaviour from others online.
- Children and young people tend to see no boundaries between on or offline life and often become victims online, through someone who knows them offline and is aware of their difficulties/impairments. In this way, the perpetrator has the knowledge to manipulate their target, especially if they have SEND.
- Although they interact less with their peers, children and young people with communication difficulties are more likely to visit gambling sites and spend more time in chat rooms. Chat rooms facilitate immediate and direct communication between users and when targeted at children and young people, are known for explicit sexual talk, innuendo, obscene language and aggressive sexual solicitations.

Additionally, this advice document notes that children and young people with SEND may be:

- More likely to believe what they're told by friends and strangers
- More trusting and have a greater belief in what they see and hear
- Less able to think critically about what they share and the consequences
- Less able to spot risky situations
- Less discriminating of both their own behaviour and the behaviour they see.

Any adaptations to our online safety provision for children with additional needs to ensure their safety online will be considered on a case by case basis and in liaison with the SENCO and the Deputy Head Pastoral.

Raising awareness on E-Safety

Children are regularly reminded of the SMART rules (Safe, Meeting, Accepting, Reliable, Tell) with posters in every Year 3 - 6 classroom 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. We use 'Smartie the Penguin' posters with younger children to teach them to tell someone when they encounter something worrying online.

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** includes assemblies followed by age-appropriate lessons in Learning for Life (PSHEE/PSED), 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.

- ➢ An agreement highlighting the acceptable use of technology is signed by parents and discussed with children.

2. How we help educate parents about online safety

Providing children at an early age with the knowledge to safeguard themselves and their personal information is crucial. However, 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.

The Manor keeps in regular contact with parents with regard to online safety, using communications to reinforce the importance of children being safe online, to explain our filtering and monitoring and to explain the online resources which children use to access their learning.

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 speakers such as **Childnet** to run parents' sessions at school, and also run further sessions led by staff at The Manor.

During Safer Internet Day and Anti-Bullying Week, we communicate with parents about how to reinforce messages about online safety and cyber-bullying at home. Resources and E-Safety guidance and updates are regularly shared with parents via newsletters and emails.

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:

Help and advice for parents and carers
Parental controls
Parents' guide to technology
Advice about key social media platforms and apps
Help for parents and carers on how to respond to online issues

3. How we train staff about online safety

Teachers are the main channel for delivering our dedicated E-Safety education in Learning for Life (PSHEE/PSED), Computing, and other curriculum lessons where technologies are being used by children and assemblies. 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.

- ➢ 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.

- ➢ All staff complete Online Safety training through EduCare.

- ➢ 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 who 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 use of technology, both within and outside school.

4. Infrastructure, filtering and monitoring

As schools increasingly work online, it is essential that children are safeguarded from potentially harmful and inappropriate online material and that filtering and monitoring systems are in place when pupils and staff access school systems and internet provisions.

The Governing Body and staff do all that they reasonably can to limit children's exposure to the above risks from the school IT system, and to fulfil their Prevent duty, by ensuring the school has appropriate filters and monitoring systems in place on school devices and school networks, and monitoring their effectiveness. This includes blocking harmful and inappropriate content without unreasonably impacting on teaching and learning, as well as ensuring that the leadership team and relevant staff have an awareness and understanding of the provisions in place and manage them effectively and know how to escalate concerns when identified. The Manor's Designated Safeguarding Lead, Head, IT Service Provider (ConnectSys) and Safeguarding Governor monitor internet usage regularly and report to the Governing Board on their findings and actions.

The Manor refers to the DfE's 'Filtering and Monitoring Standards' to support us in this area, with the Designated Safeguarding Lead taking the lead role in ensuring we meet these standards. Filtering and monitoring provision is reviewed regularly, and is formally discussed with the Safeguarding Governor on at least a termly basis. The full Governing Board reviews this area at least annually.

Please see Appendix 1 for details of our infrastructure, filtering and monitoring, which is via our 'Securly' and 'Sophos' systems. Our 'Securly' platform automatically sends alerts regarding any concerning content or online behaviour to the Deputy Head Pastoral (who is the Designated Safeguarding Lead). They will then support children accordingly in liaison with the relevant pastoral staff and also take steps to add policies to our filtering and monitoring system, ‘Securly’, to ensure any inappropriate content cannot be accessed again.

The school supplements filters with behaviour management and supervision of children online. If staff have any concerns in relation to filtering and monitoring, these must be reported to the Designated Safeguarding Lead.

Whilst considering our responsibility to safeguard and promote the welfare of children, and provide them a safe environment in which to learn, the school considers the age range of the pupils, the number of pupils, how often they access the school’s IT system and the proportionality of costs vs risks.

The School also consults the UK Safer Internet Centre for guidance as to what “appropriate” filtering might look like:

- UK Safer Internet Centre: appropriate filtering and monitoring

Whilst the Governing Body and staff ensure that appropriate filters and monitoring systems are in place, the School takes care that “over blocking” does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding.

The Manor Preparatory School acknowledges that whilst filtering and monitoring is an important part of the school’s online safety responsibilities, it is only one part of our approach to online safety. Pupils and adults may have access to systems external to the school control such as mobile phones and other internet enabled devices and technology and where concerns are identified, appropriate action will be taken in line with our Safeguarding policy.

Information Security and Access Management

The Manor recognises that education settings are directly responsible for ensuring they have the appropriate level of security protection procedures in place in order to safeguard their systems, staff and learners and review the effectiveness of these procedures periodically to keep up with evolving cyber-crime technology.

Guidance on e-security is available from the National Education Network. The Manor also refers to the DfE Cyber security standards for schools and colleges. Broader guidance on cyber security, including considerations for Governors, can be found at Cyber security training for school staff - NCSC.GOV.UK.

5. Reporting mechanisms available for all users to report issues and concerns to the school and how they are managed and/or escalated

If any member of the school community has an online safety concern which is of a Safeguarding nature, including Child-on-Child Abuse and Sexual Violence and Harrassment, this should be reported to the Deputy Head Pastoral as Designated

Safeguarding Lead, or a deputy DSL, in line with the procedures outlined in our Safeguarding Policy.

If a child is the victim of Cyber-bullying or any unkind online behaviour, 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. In cases of Cyber-bullying, we advise children to:

- Save any evidence of the bullying and show an adult
- Block messages or the person and do not respond to them in any way
- Log off the site where the cyberbullying is happening
- Talk to someone you trust about it (trusted adults at home and staff)

Parents aware of Cyber-bullying or misuse of the internet by a child should inform their child's Head of Section and/or Deputy Head Pastoral.

Teachers aware of Cyber-bullying or misuse of the internet by a child should inform their Head of Section and the Deputy Head Pastoral.

Where concerns about Cyber-bullying or misuse of the internet have been raised, the Head of Section and Deputy Head Pastoral will then investigate the matter, support the children and where appropriate, issue sanctions in line with the process outlined in our Anti-Bullying Policy, keeping the Head informed throughout this process. We always continue to monitor reported incidents. Bullying on the basis of protected characteristics is taken particularly seriously and we distinguish incidents of this type of bullying in our records.

If the concern is of a Safeguarding nature, including Child-on-Child Abuse and Sexual Violence and Sexual Harassment, this should only be reported to the Deputy Head Pastoral as Designated Safeguarding Lead, or a deputy, in line with our Safeguarding Policy.

The Manor is aware that the sharing of nude and semi-nude images, as well as sexting, between children and young people is illegal, although we recognise that children and young people should not be unnecessarily criminalised. Should staff become aware of any such incidents, this should be reported to the Designated Safeguarding Lead or a deputy who will manage these in line with our Safeguarding Policy. The Manor educates pupils about the dangers of sexting and how to seek support through Learning for Life (PSHEE/PSED) and Computing lessons. Please refer to our Safeguarding Policy for further information on this issue.

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. If a member of staff suspects that a child has used a mobile phone inappropriately, they should contact the Deputy Head Pastoral in the first instance for advice. In discussion with the Deputy Head Pastoral and the Head, staff may examine the mobile phone although staff must be aware that they must not view or forward illegal images of a child. Further information about this process and what to do when viewing an image is unavoidable can be found in the 'searching screening and confiscation advice (for schools)' and 'Sharing nudes and semi-nudes: advice for education settings working with children and young people', as well as in The Manor's Safeguarding Policy.

The School has the right to intervene in pupils' user accounts and files if they are suspected of being unsuitable. 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 sign an age-appropriate 'home-school' agreement, agreeing to responsible use of the internet. This is also discussed with pupils.

SECTION C – Cyber-bullying

Please also see the school's Anti-bullying Policy

The School also pays heed to the DfE guidance and supplementary advice documents below:

- Behaviour in Schools (DfE, September 2022)
- Preventing and Tackling Bullying (DfE, July 2017)
- Cyberbullying: Advice for Headteachers and School Staff (DfE, November 2014).
- Advice for parents and carers on cyberbullying (DfE, November 2014)

Definition of Cyber-bullying

Cyber-bullying, or online bullying, can be defined as the use of technologies by an individual or by a group of people to deliberately and repeatedly upset someone else. (Childnet - "Cyberbullying Guidance")

Cyberbullying can include discrimination and hate crimes, including sexist bullying, racist and faith targeted bullying, bullying related to sexual orientation (homophobic or biphobic bullying), bullying related to gender identity (transphobic bullying) and bullying of people because they have special educational needs and disabilities

Cyber-bullying, like other forms of bullying, affects self-esteem and self-confidence and can affect mental health and wellbeing, in the worst cases leading to self-harm and suicide. Addressing all forms of bullying and discrimination is vital to support the health and wellbeing of all members of the school community.

Cyber-bullying takes different forms: threats and intimidation; harassment or stalking (e.g. repeatedly sending unwanted texts or instant messages); vilification and defamation; ostracism and peer rejection; impersonation; and forwarding or publically posting private information or images.

Cyber-bullying can be characterised in several specific ways that differ from face-to-face bullying. These include the profile of the person carrying out the bullying; the location of online bullying; the potential audience; the perceived anonymity of the person cyber-bullying; motivation of the person cyber-bullying; and the digital evidence of cyber-bullying.

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. The Governing Board strategically review and monitor The Manor's online safety provision in liaison with the Head, the Deputy Head

Pastoral, the Deputy Head Academic and the Head of Pre-Prep. 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 Learning for Life (PSHEE/PSED) Subject Leader ensures online safety and issues such as Cyber-bullying are addressed in the Learning for Life curriculum.
- the Manor's IT Service Provider (ConnectSys) is responsible for ensuring firewalls and other systems are enabled to filter internet usage and monitor pupils' internet use.
- The Designated Safeguarding Lead (Deputy Head Pastoral) takes lead responsibility for safeguarding and child protection, including online safety and understanding the filtering and monitoring systems and processes in place.

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

Please also see Section A and B of this policy for pupils in relation to Computing, mobile phones and electronic devices, as well as information on our technical infrastructure and how this filters and monitors inappropriate content. 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.

Our Deputy Head Pastoral (as Designated Safeguarding Lead) also monitors user activity online and works with our technical support staff to maintain effective filtering and monitoring systems. This includes responding to alerts sent to the Deputy Head Pastoral whenever inappropriate content is flagged by our 'Securly' monitoring system. The Deputy Head Pastoral meets regularly with the Head and Safeguarding Governor on matters of filtering and monitoring to ensure we continually review this area. An annual review of filtering and monitoring at The Manor also takes place with the Senior Leadership Team (including the Deputy Head Pastoral), IT Service Provider, Computing leads and Safeguarding Governor in attendance.

If pupils are found to be using the internet in an unacceptable manner, the school's Behaviour, Discipline and Exclusion 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 sanctions from the school, in line with our Behaviour, Discipline and Exclusion Policy and Anti-Bullying Policy.

Mobile Phones (Pupils)

The Manor Preparatory School recognises the specific risks that can be posed by mobile phones and cameras and in accordance with KCSIE 2024 and the EYFS Statutory Framework 2023, has appropriate policies in place that are shared and understood by all members of the school community.

Pupils are not permitted to bring mobile phones to school, although pupils on the school Joint Bus Service buses 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. The Manor recognises that during the coach /minibus journey, children may have unlimited access to the internet via mobile phone networks (i.e. 3G, 4G and 5G). This access means that some children may sexually harass their peers via their mobile and smart technology, share indecent images: consensually and non-consensually (often via large chat groups), and view and share pornography and other harmful content. To mitigate this risk, children from The Manor are sat at the front of JBS buses, where it is easier for them to be supervised. We tell the children not to use their mobile phones unless they are contacting a parent, and any concerns raised by JBS staff will be passed on to the Deputy Head Pastoral, to be followed up on by The Manor.

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 Governing Board, Head, Deputy Head Pastoral, Head of Computing and Learning for Life (PSHEE/PSED) Subject Leader ensures that the issue of Cyber-bullying is regularly addressed in the curriculum lessons in Key Stages 1 & 2, including reinforcing with children the importance of ensuring that any online communication is kind and respectful.

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. The key message given to pupils is: if you encounter anything online that you find upsetting, you should tell a trusted adult at home and/or a member of staff.

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. Children in the Early Years 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.

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) and the Staff Behaviour Policy). All new staff are given guidance on the school’s policy on camera and mobile phone use, and taking, using and storing images of children, also contained within the Acceptable Use Policy (For Staff) and the Safeguarding Policy.

Online safety and cyber-bullying is built into our staff training schedule, ensuring staff have 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 a child is the victim of Cyber-bullying or any unkind online behaviour, 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. In cases of Cyber-bullying, we advise children to:

- Save any evidence of the bullying and show an adult
- Block messages or the person and do not respond to them in any way
- Log off the site where the cyberbullying is happening
- Talk to someone you trust about it (trusted adults at home and staff)

Parents aware of Cyber-bullying or misuse of the internet by a child should inform their child’s Head of Section and/or Deputy Head Pastoral.

Teachers aware of Cyber-bullying or misuse of the internet by a child should inform their Head of Section and the Deputy Head Pastoral.

Where concerns about Cyber-bullying or misuse of the internet have been raised, the Head of Section and Deputy Head Pastoral will then investigate the matter, support the children and where appropriate, issue sanctions in line with the process outlined in our Anti-Bullying Policy, keeping the Head informed throughout this process. We always continue to monitor reported incidents. Bullying on the basis of protected characteristics is taken particularly seriously and we distinguish incidents of this type of bullying in our records.

If the concern is of a Safeguarding nature, including Child-on-Child Abuse and Sexual Violence and Sexual Harassment, this should only be reported to the Deputy Head Pastoral as Designated Safeguarding Lead, or a deputy, in line with our Safeguarding Policy.

The Manor is aware that the sharing of nude and semi-nude images, as well as sexting, between children and young people is illegal, although we recognise that children and young people should not be unnecessarily criminalised. Should staff become aware of any such incidents, this should be reported to the Designated Safeguarding Lead, who will manage these in line with our Safeguarding Policy. The

Manor educates pupils about the dangers of sexting and how to seek support through Learning for Life (PSHEE/PSED) and Computing lessons. Please refer to our Safeguarding Policy for further information on this issue.

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. If a member of staff suspects that a child has used a mobile phone inappropriately, they should contact the Deputy Head Pastoral in the first instance for advice. In discussion with the Deputy Head Pastoral and the Head, staff may examine the mobile phone although staff must be aware that they must not view or forward illegal images of a child. Further information about this process and what to do when viewing an image is unavoidable can be found in the 'searching screening and confiscation advice (for schools)' and 'Sharing nudes and semi-nudes: advice for education settings working with children and young people', as well as in The Manor's Safeguarding Policy.

The School has the right to intervene in pupils' user accounts and files if they are suspected of being unsuitable. 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). The Manor's filtering and monitoring system, 'Securly', ensures that any communication and internet use on school devices and platforms is monitored and any concerns are immediately flagged to the Deputy Head Pastoral.

Parents sign an age-appropriate 'home-school' agreement, agreeing to responsible use of the internet. This is also discussed with pupils.

f. Informing and educating parents and carers in online safety

We advise parents in letters about the risks 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 and our own staff. Parents are encouraged to report any concerns regarding inappropriate internet sites or communication to the school and, where appropriate, 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.

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

Please see the school's Data Protection Policy.

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

Please see Section B of this policy.

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

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
- 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)
- 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
- Do not download or install programs or applications to the school's IT equipment
- Understand that the school monitors your internet use and the sites that you visit and that your internet access is filtered at all times. You should not try to access sites if you know that they are not allowed.

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. We use Chromebooks and iPads for learning and not for playing games.
- Take good care of all IT hardware at all times
- Do not eat or drink near IT equipment
- 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

Remember that 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.

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. Please note that where visitors have access to The Manor's devices or internet, they will use a restricted guest account which does not allow access to any school data.

Guidance for pupils can be found 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, Safeguarding Policy, Staff Behaviour 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 online 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.
- 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
- 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. Any such requests should be reported to the Head.
- 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
- Staff members must not have contact through any personal social media with:
  - any current pupils, whether from the School or any other school, unless 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 or the Director of Admissions, Marketing and Communication 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 online 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 should 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 will use internet searches to perform due diligence on shortlisted candidates in the course of recruitment, in accordance with Keeping Children Safe in Education 2024. 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

The leadership team has 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.

If you become aware of a breach of this Acceptable Use 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.

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 Service Provider (ConnectSys) or Director of Finance and Operations.

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 Director of Finance and Operations.

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 and filtered 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 (e.g. CPOMS) 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 Director of Finance and Operations.

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 devices 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.

SECTION F – Remote Learning

Please also see the Remote Teaching and Learning Policy.

The Manor Preparatory School acknowledges that where children are being asked to learn online at home the department has provided advice to support schools to do so safely. The Manor complies with Keeping Children Safe in Education 2024, which states:

138. Guidance to support schools and colleges understand how to help keep pupils, students and staff safe whilst learning remotely can be found at Safeguarding and remote education - GOV.UK (www.gov.uk) and Providing remote education: guidance for schools - GOV.UK (www.gov.uk).

139. Schools and colleges are likely to be in regular contact with parents and carers. Those communications should be used to reinforce the importance of children being safe online and parents and carers are likely to find it helpful to understand what systems schools and colleges use to filter and monitor online use. It will be especially important for parents and carers to be aware of what their children are being asked to do online, including the sites they will be asked to access and be clear who from the school or college (if anyone) their child is going to be interacting with online.

SAFEGUARDING CHILDREN REMOTELY

It is important that all staff who interact with children, including online, continue to look out for signs a child may be at risk. Any such concerns should be dealt with as per the Safeguarding Policy by contacting the DSL or a Deputy DSL as soon as possible and following up with a written report of the concern (please see Safeguarding Policy for details) and where appropriate referrals should still be made to children's social care and as required, the police.

Remote Lessons
At The Manor, remote learning will be offered through our secure Google Classroom virtual learning environment. Activities for children to complete will be made available on Google Classroom by teachers and children will be able to join the lesson from home via webcam.

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

The below rules must be followed when delivering virtual lessons, especially where webcams are involved:

- Staff and children must wear suitable clothing, as should anyone else in the household
- Any computers used should be in appropriate areas, for example, not in bedrooms; and the background should be blurred
- The live class should be recorded so that if any issues were to arise, the video can be reviewed
- Live classes should be kept to a reasonable length of time

● Language must be professional and appropriate, including any family members in the background
● Staff must only use platforms provided by The Manor Preparatory School to communicate with pupils
● The length, time, date and attendance of any sessions held will be automatically recorded by our Google learning platform.

The DSL will monitor any online safety issues that arise, including via our filtering and monitoring systems, and communicate actions to be taken to staff, children and parents to help educate and protect them from these issues.

Supporting Children Not in School

The Manor Preparatory School is committed to ensuring the safety and wellbeing of all its children. Where children remain at home, regular contact will be made with these families by teachers to offer support and guidance for their pastoral care and learning.

Where the DSL has identified a child to be on the edge of social care support, or who would normally receive pastoral-type support in school, they should ensure that a robust communication plan is in place for that child or young person. The communication plans can include; remote contact, phone contact and door-step visits. Other individualised contact methods should be considered and recorded.

The Manor Preparatory School and its DSL will work closely with all stakeholders to maximise the effectiveness of any communication plan. This plan must be reviewed regularly (at least once a fortnight) and where concerns arise, the DSL will consider any referrals as appropriate.

The DSL and DDSL's will meet on a weekly basis to discuss concerns and actions taken to support children. They will meet with the Safeguarding governor regularly to discuss and review cases and procedures. The Manor Preparatory School recognises that school is a protective factor for children and young people, and where children are accessing learning remotely, this can affect the mental health of children and their parents/carers. Children will be given regular opportunities to express their feelings with staff using the above communication lines. Teachers at our school need to be aware of the children's mental health in setting expectations of pupils' work where they are at home.

Use of Electronic Equipment for Remote Learning during School Closure

In the case of school closure, Chromebooks will be issued to children in Years 3 to 6 and the following precautions will apply for the use of this technology for remote learning:

1. **Year 3 - 6 Loan of School Chromebooks**

   1.1 Ownership of Chromebooks
   School Chromebooks are loaned to children in Years 3 - 6.

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 Chromebooks Agreements

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 Service Provider (ConnectSys). 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.
- 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.

- Filter and monitor the children’s activity on their school Chromebooks and school Google accounts, via our ‘Securly’ system. 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 and Acceptable Use Policy 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 or concerns arising from their Chromebook use so that the IT Service Provider and/or Deputy Head Pastoral 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 Director of Finance and Operations and/or Deputy Head Pastoral about any security problems or other concerns arising from their child’s Chromebook use that 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.

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 licence 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, Discipline and Exclusions 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:

- Record of serial number
- The Manor Fixed Asset Number

8. Repair and Replacement of Chromebooks

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.** In these cases, the cost of repairs or replacement Chromebooks will be paid for by parents. 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 Service Provider as soon as it occurs.

9. The Manor Chromebook Home-School Agreement

Parents sign a home-school agreement to confirm that they agree to the above conditions when children are loaned a Chromebook by The Manor Preparatory School for their learning.

APPENDIX 1 - CONTENT FILTERING

Content Filtering – Securly – Web filter for schools

Securly Web Filter is a cloud-based filtering solution designed primarily for schools to ensure safe and secure internet access for students. It helps schools manage and monitor online activity by filtering out inappropriate, harmful, or distracting content. Below are some key features and functionalities of Securly Web Filter:

1. Content Filtering

- Securly uses AI and machine learning to filter out inappropriate content such as violence, adult content, and hate speech.
- The filter can be customised to block specific categories, websites, or content types based on school policies.

2. Cloud-Based Filtering

- As a cloud-based solution, Securly Web Filter works across various devices, whether they're on or off the school network.
- This ensures consistent filtering policies whether students are in school, at home, or using mobile devices.

3. Real-Time Monitoring

- The filter provides real-time alerts to school administrators if students engage in risky online behaviour, such as accessing harmful content or showing signs of self-harm, cyberbullying, or other dangerous activities.

4. Reporting and Analytics

- Detailed reports can be generated to track students' online activities, showing which sites they are visiting, what content is being blocked, and potential security risks.
- These reports can be used to review trends, understand student behaviour, and enhance digital learning environments.

5. Parental Controls

- Securly offers parental controls that allow parents to monitor their child's internet use at home, ensuring safety beyond school hours.

6. Compliance

- Securly Web Filter is compliant with legal standards like the Children's Internet Protection Act (CIPA), ensuring that schools meet the required guidelines for safe internet usage.

Securly’s Safe Search feature enhances student online safety by filtering and restricting search engine results to prevent access to inappropriate content. It integrates with popular search engines like Google, Bing, and YouTube to ensure that search results align with school policies. Securly Safe Search works as follows:

1. Search Term Filtering

- Securly automatically filters out specific keywords or phrases that could lead to inappropriate or harmful content.

- If a student searches for terms that are flagged as unsafe, the Safe Search filter blocks the results or redirects the search.

2. Enforced Safe Search Mode

- Securly forces the Safe Search mode on search engines like Google and Bing, meaning students only receive filtered results.

- This setting prevents students from disabling Safe Search or bypassing the filter.

3. Content Analysis

- The Safe Search feature uses AI to analyse search results and block any images, videos, or websites that contain inappropriate content, even if they slip through the search engine’s own filtering mechanisms.

- This ensures that even if a keyword seems safe, harmful content is still filtered out.

4. YouTube Restricted Mode

- Securly can enforce YouTube’s Restricted Mode, which limits access to inappropriate videos and filters out potentially harmful content in comments and recommendations.

- This mode helps in preventing access to age-inappropriate videos or those with violent or adult content.

- This mode also restricts access to comments, which can sometimes contain harmful or offensive language.

- Additionally, Securly’s AI analyses video titles, descriptions, and metadata to detect and block inappropriate content even if it’s not explicitly labelled as such.

5. Customisable Safe Search Settings

- School administrators can customise Safe Search settings according to their specific needs. They can block additional categories, specific websites, or even create exceptions based on educational needs.

6. Reporting and Alerts

- If a student attempts to search for restricted content, Securly generates reports and can send real-time alerts to administrators.
- This helps in tracking patterns of risky behaviour and provides insights for intervention if necessary.

7. Compatibility Across Devices

- The Safe Search feature works on all devices used by students, whether they are Chromebooks, laptops, or mobile devices, ensuring consistent filtering across all platforms.

In summary, Securly Web Filter is a comprehensive web filtering and monitoring solution aimed at providing a safe online environment for students, ensuring they can use the internet for learning while being protected from harmful or inappropriate content.

Email Filtering

Sophos Cloud Email is a cloud-based email security solution designed to protect organisations from email-borne threats like phishing, malware, ransomware, and spam. It integrates with popular email platforms such as Microsoft 365 and Google Workspace, offering comprehensive protection without the need for complex on-premise hardware or software.

1. Advanced Threat Protection

- Sophos Cloud Email leverages multi-layered security to detect and block known and zero-day threats. It uses a combination of machine learning, behavioural analysis, and threat intelligence to prevent phishing, spear-phishing, and malware attacks.

2. Anti-Spam and Anti-Phishing

- The solution includes robust anti-spam and anti-phishing filters that identify and block malicious emails, ensuring that harmful content doesn't reach users' inboxes.
- Sophos also provides impersonation protection to detect and block Business Email Compromise (BEC) attempts.

3. Email Encryption and Data Loss Prevention (DLP)

- Sophos Cloud Email includes encryption features to secure sensitive information sent via email, ensuring compliance with regulations like GDPR and HIPAA.
- It also offers Data Loss Prevention (DLP) policies that can automatically block or quarantine emails containing sensitive information based on predefined rules.

4. Sandboxing for Zero-Day Threats

- Suspicious email attachments are automatically sent to a secure sandbox environment where they are analysed for malicious behaviour. This protects against unknown or emerging threats.

5. Easy Integration with Email Platforms

- The solution seamlessly integrates with popular cloud email platforms like Microsoft 365 and Google Workspace, providing continuous protection without requiring additional hardware or complex configurations.

6. User Awareness and Training

- Sophos Cloud Email includes tools to help train users to recognise phishing attacks. Simulated phishing campaigns can be sent to educate employees and improve overall security awareness.

7. Centralised Management and Reporting

- Administrators can manage all email security policies, monitor threats, and generate detailed reports from a centralised dashboard. This unified management makes it easier to track threats and enforce compliance.

8. Automated Threat Response

- Sophos Cloud Email can automatically quarantine or delete malicious emails based on predefined rules. It also provides actionable alerts and insights to help administrators respond quickly to incidents.

9. Business Continuity and Archiving

- The solution offers email continuity services to ensure that email communication continues even if the primary email server is down.
- It also provides archiving options, ensuring that important email communications are securely stored and easily retrievable.

Sophos Cloud Email is a comprehensive and scalable email security solution that provides advanced protection against modern email-based threats. With features like AI-driven threat detection, encryption, DLP, and seamless integration with cloud email platforms, it’s designed to enhance security, compliance, and productivity for organisations of all sizes.