ONLINE 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 2025
Date of next review:	1 September 2026
Person(s) responsible for review:	SLT (DH Pastoral)

Contents

1. AIMS

The Manor aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Identify and support groups of pupils that are potentially at greater risk of harm online than others
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

Our approach to online safety is based on addressing the following four key categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as 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, such as 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

2. LEGISLATION AND GUIDANCE

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on

pupils' electronic devices where they believe there is a 'good reason' to do so.

3. ROLES AND RESPONSIBILITIES

The Governing Board

The governing board has overall responsibility for monitoring this policy and holding the Head and Deputy Head Pastoral to account for its implementation.

The governing board will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

The governing board will also make sure all staff receive regular online safety updates (for example, via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, requirements for training, and monitor online safety logs as provided by the Designated Safeguarding Lead (DSL). This takes place on at least a termly basis in meetings between the Safeguarding Governor and the Deputy Head Pastoral, who is also the DSL.

The governing board should ensure children are taught how to keep themselves and others safe, including keeping safe online.

The governing board must ensure The Manor has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The board will review the DfE's filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting the standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
- Reviewing filtering and monitoring provisions at least annually;
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning;
- Having effective monitoring strategies in place that meet their safeguarding needs.

The governor who oversees online safety is the Safeguarding Governor, Mr Mark Skidmore.

All governors will:

- Ensure they have read and understand this policy
- Agree and adhere to the terms on acceptable use of The Manor's ICT systems and the internet (Appendix B)
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole-school approach to safeguarding and related policies and/or procedures
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special

educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

The Head and Deputy Head Pastoral

The Head and Deputy Head Pastoral are responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

The Deputy Head Pastoral (Designated Safeguarding Lead)

The Designated Safeguarding Lead (DSL) at The Manor is Mr Varun Footring and further details about this role and that of the Deputy DSLs are set out in our Safeguarding Policy, including a job description.

The DSL takes lead responsibility for online safety at The Manor, in particular:

- Supporting the Head in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the Head and governing board to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Providing governors with assurance that filtering and monitoring systems are working effectively and reviewed regularly
- Working with the school's IT provider, ConnectSys, to make sure the appropriate systems and processes are in place
- Working with the Head, ConnectSys and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with The Manor's Safeguarding Policy
- Responding to safeguarding concerns identified by filtering and monitoring
- Ensuring that any online safety incidents are logged on CPOMS and/or The Manor's separate Filtering and Monitoring Incident Log, and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with The Manor's Behaviour, Discipline and Exclusion Policy, Anti-Bullying Policy, Safeguarding Policy and Section 6 of this Online Safety and Acceptable Use Policy.
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the Head and the Governing Board
- Undertaking annual risk assessments that consider and reflect the risks children face

- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

This list is not intended to be exhaustive.

The Manor's IT Provider (ConnectSys)

The Manor's IT Provider (ConnectSys) is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that The Manor's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a regular basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- In liaison with the Deputy Head Pastoral, ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- In liaison with the Deputy Head Pastoral, ensure that any incidents of cyber-bullying are dealt with appropriately in line with The Manor's Behaviour, Discipline and Exclusion Policy, Anti-Bullying Policy, Safeguarding Policy and Section 6 of this Online Safety and Acceptable Use Policy.

This list is not intended to be exhaustive.

All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (Appendix B), and ensuring that pupils follow the school's terms on acceptable use (Appendix A)
- Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing by reporting the matter to the DSL or a Deputy DSL immediately and then logging notes of the incident on CPOMS
- Following the correct procedures by contacting ConnectSys if they need to bypass the filtering and monitoring systems for educational purposes
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line The Manor's Behaviour, Discipline and Exclusion Policy, Anti-Bullying Policy, Safeguarding Policy and Section 6 of this Online Safety and Acceptable Use Policy.

- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'

This list is not intended to be exhaustive.

Parents/carers

Parents/carers are expected to:

- Notify a member of staff, the Deputy Head Pastoral or the Head of any concerns or queries regarding this policy
- Ensure their child has read and understood the terms on acceptable use of the school's ICT systems and internet (Appendix A)

Parents/carers can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? – UK Safer Internet Centre
- Online safety topics for parents/carers – Childnet
- Parent resource sheet – Childnet

Visitors and members of the community

Visitors and members of the community who use The Manor's ICT systems or internet will be made aware of this policy and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (Appendix B).

4. EDUCATING PUPILS ABOUT ONLINE SAFETY

Pupils will be taught about online safety as part of the curriculum. This includes the areas specified in the DfE's guidance on relationships education, relationships and sex education (RSE) and health education.

In Years 1 and 2, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

In Years 3 to 6, pupils will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact
- Be discerning in evaluating digital content

By the end of Year 6, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not

- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online, including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information, including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know
- The benefits of rationing time spent online, the risks of excessive time spent on electronic devices and the impact of positive and negative content online on their own and others' mental and physical wellbeing
- How to consider the effect of their online actions on others and know how to recognise and display respectful behaviour online and the importance of keeping personal information private
- Where and how to report concerns and get support with issues online

In Years 1-6, we follow the Rising Stars 'Switched On Online Safety' scheme of work in Computing lessons. 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 refer to our Learning for Life (PSHEE/PSED) Policy and RSHE (Relationships, Sex and Health Education) Policy for further information.

The safe use of social media and the internet will also be covered in other subjects where relevant.

Pupils will also receive age-appropriate training on safeguarding issues such as cyberbullying and the risks of online radicalisation.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

5. EDUCATING PARENTS/CARERS ABOUT ONLINE SAFETY

The Manor will raise parents/carers' awareness of internet safety through regular letters in the Weekly Mailing and in online safety guidance available on the Parent Portal. This topic is also addressed within parent talks over the course of the year as appropriate, and external speakers such as Childnet also deliver parent talks at least biennially. This policy will also be shared with parents/carers.

The Manor will let parents/carers know:

- What systems The Manor uses to filter and monitor online use

- What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online

If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the Deputy Head Pastoral or Head. Questions about the curriculum may also be directed to the Head of Computing, Mrs Fiona Mullaney, or the Pre-Prep Computing Coordinator, Mrs Emma Gower.

6. CYBER-BULLYING POLICY

Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. The Manor recognises that bullying behaviour does not need to be repeated over time for us to take action. See also The Manor's Anti-Bullying Policy, Behaviour, Discipline and Exclusion Policy and Safeguarding Policy.

Preventing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The Manor will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Form Teachers discuss this topic with their forms as part of our Learning for Life (PSHEE/PSED) curriculum and it is also addressed in Computing lessons and during the whole-school focus on Anti-Bullying Week.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum in other subjects to cover cyber-bullying, where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

The Manor also sends information/leaflets on cyber-bullying to parents/carers so they are aware of the signs, how to report it and how they can support children who may be affected.

Dealing with an incident of cyber-bullying

In relation to a specific incident of cyber-bullying,The Manor will follow the processes in the Anti-Bullying Policy and below. Where illegal, inappropriate or harmful material has been spread among pupils, The Manor will use all reasonable endeavours to ensure the incident is contained.

The Deputy Head Pastoral as DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

If a pupil 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. In cases of cyber-bullying, we advise pupils 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 they trust about it (trusted adults at home and staff at school)

Parents who become aware of cyber-bullying or misuse of the internet by a child should inform their child's Form Teacher, Head of Section and/or the Deputy Head Pastoral.

Staff who become 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 DSL, 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 DSL, who will manage these in line with our Safeguarding Policy.

The Manor has the right to intervene in pupils' user accounts and files if they are suspected of being unsuitable. The Manor, 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 in relation to 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.

Examining electronic devices

The Head, and any member of staff authorised to do so by the Head (the Deputy Head Pastoral, Head of Pre-Prep, Deputy Head Academic and Heads of Section), can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- Is identified as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the Head.
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's co-operation

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL and the Head to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent/carer refuses to delete the material themselves

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image
- Confiscate the device and report the incident to the DSL or a Deputy DDSL immediately, who will decide what to do next. The DSL or deputy will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through The Manor's complaints procedure.

Artificial intelligence (AI)

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Gemini.

The Manor recognises that AI has many uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.

The Manor will treat any use of AI to bully pupils very seriously, in line with our Anti-Bullying Policy and Behaviour, Discipline and Exclusion Policy.

Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used by the school, and where existing AI tools are used in cases which may pose a risk to all individuals that may be affected by it, including, but not limited to, pupils and staff.

The Department has published Generative AI: product safety expectations to support schools to use generative artificial intelligence safely, and explains how filtering and monitoring requirements apply to the use of generative AI in education.

7. ACCEPTABLE USE OF THE INTERNET IN SCHOOL

All pupils, parents/carers, staff, volunteers and governors are expected to act in accordance with the acceptable use of the school's ICT systems and the internet:

- Year 1-6 pupils 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 online safety lessons.
- Parents of new pupils joining The Manor sign an electronic agreement on entry to confirm they have read the Online Safety and Acceptable Use Policy and discussed this with their child.
- Staff confirm their agreement with the Acceptable Use Policy via an annual safeguarding survey.

Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above and restrict access through filtering systems where appropriate.

More information is set out in the acceptable use policies in appendices A and B

8. PUPILS USING MOBILE DEVICES IN SCHOOL

Pupils are not permitted to bring mobile phones to school, although pupils on the school Joint Bus Service 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 journey. The Manor recognises that during the coach journey, children may have unlimited access to the internet via mobile phone networks. To mitigate this risk, 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 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.

9. STAFF USING WORK DEVICES OUTSIDE SCHOOL

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords can be made up of three random words, in combination with numbers and special characters if required, or generated by a password manager
- Not sharing the device among family or friends
- Making sure the device locks if left inactive for a period of time
- ConnectSys will ensure that anti-virus and anti-spyware software is installed on all staff work devices
- ConnectSys will ensure that hard drives are encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- ConnectSys will keep operating systems up to date by always installing the latest updates

Staff members must not use the device in any way that would violate The Manor's terms of acceptable use.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from ConnectSys.

10. PARENT/CARER USE OF CAMERAS, RECORDING EQUIPMENT, MOBILE DEVICES AND OTHER DEVICES WITH IMAGING AND SHARING CAPABILITIES

Parents/carers are not allowed to use mobile phones, cameras or other devices with imaging and sharing capabilities where EYFS children are present.

Parents/carers are welcome to take photographs of their own children taking part in outdoor and sporting events except swimming, where no photography/video of any description is allowed. When an event is held indoors, such as a play or a concert, parents/carers should be mindful of the need to use their cameras and recording devices with consideration and courtesy for the comfort of others.

We ask parents/carers not to take close-up photographs of other pupils who are on their own, without the prior agreement of that child's parents. Group photos where their child is the main subject of the photograph are acceptable.

Parents/carers must not upload any images, moving or still, other than those of their own child, onto social media sites (this includes photographs of members of staff or other adults).

Parents/carers may not use any mobile phones, cameras or other devices with imaging and sharing capabilities in changing rooms or backstage, nor to any areas where photography or filming may embarrass or upset pupils.

Parents/carers are also reminded that copyright issues may prevent us from permitting the filming or recording of some plays and concerts.

11. STAFF USE OF CAMERAS, RECORDING EQUIPMENT, MOBILE DEVICES AND OTHER DEVICES WITH IMAGING AND SHARING CAPABILITIES

EYFS

Early Years staff are not permitted to have personal mobile phones, cameras or other devices with imaging and sharing capabilities in the classroom – they must be kept in a designated staff area or a locked cupboard during the school day. Early Years staff are only permitted to use their own phones for calls during their breaks and in a place where children are not present.

On Early Years' outings/trips, a school mobile telephone should be taken, for emergency contact. If members of staff take their own mobile phones on outings/trips, for use in case of an emergency, they must not make or receive personal calls. Members of staff will not use their personal mobile phones, cameras or other devices with imaging and sharing capabilities for taking photographs of children on outings/trips.

Whole School

Members of staff may not use a personal phone, camera or other device with imaging and sharing capabilities to take photographs of pupils in or outside school. They should instead use school-provided devices.

The only exception to this is if the staff member is also a parent at the school and the primary subject of the photograph is their own child.

No mobile phones, cameras or other electronic devices imaging and sharing capabilities should be taken into changing areas or toilet areas.

Any personal calls should be made at staff breaks or in non-contact lessons and in a place where children are not present. A school landline may also be used.

Staff need to check with the Marketing and Admissions Assistant about using any photographs of children whose parents have requested that their images should not be used for any purposes.

Anyone found to be in breach of this policy will face the possibility of disciplinary action.

12. HOW THE MANOR WILL RESPOND TO ISSUES OF MISUSE

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our Behaviour, Discipline and Exclusion Policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the Disciplinary Policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The Manor will consider whether incidents that involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

13. TRAINING

Staff, governors and volunteers

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues, including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
  - Abusive, threatening, harassing and misogynistic messages
  - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
  - Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse

- Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks
- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL and DDSLs will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our Safeguarding Policy.

14. MONITORING ARRANGEMENTS

The Deputy Head Pastoral logs behaviour and safeguarding issues related to online safety.

This policy will be reviewed every year by the Deputy Head Pastoral. At every review, the policy will be shared with the Head and the governing board. The review will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

15. LINKS WITH OTHER POLICIES

This policy is linked to our:

- Safeguarding Policy
- Behaviour, Discipline and Exclusion Policy
- Anti-Bullying Policy
- Disciplinary Policy
- Data Protection Policy
- Complaints Policy

APPENDIX A: 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:

- Courage
- Perseverance
- Kindness
- Respect
- Creativity
- Unity

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.

APPENDIX B: ACCEPTABLE USE POLICY (STAFF, GOVERNORS AND VISITORS)

In this policy, the term 'staff' covers staff, governors and visitors.

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. Any staff member(s) suspected of committing a breach of this Policy will be required to co-operate with The Manor'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.

Use of The Manor's ICT systems and internet

When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), staff must not:

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material)
- Use them in any way that could harm the school's reputation
- Access social networking sites or chat rooms
- Use any improper language when communicating online, including in emails or other messaging services
- Install any unauthorised software, or connect unauthorised hardware or devices to the school's network
- Share passwords with others or log in to the school's network using someone else's details
- Take photographs of pupils without checking with teachers first
- Share confidential information about the school, its pupils or staff, or other members of the community
- Access, modify or share data they are not authorised to access, modify or share
- Promote private businesses, unless that business is directly related to the school

Staff must only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of their role.

The Manor will monitor the websites staff visit when on the school network, and their use of the school's ICT facilities and systems.

Staff must take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's Data Protection Policy.

Staff must let the Designated Safeguarding Lead (DSL) know if a pupil informs them they have found any material that might upset, distress or harm them or others, and must also do so if they encounter any such material themselves.

Staff must always use the school's ICT systems and internet responsibly, and ensure that pupils in their care do so too. Any property belonging to the School should be treated with respect and care, and used only in accordance with any training and policies provided. Staff must report any faults or breakages without delay to the IT Service Provider (ConnectSys) or Director of Finance and Operations.

Where staff use personal devices for work purposes, they must ensure they comply with The Manor's Bring Your Own Device Policy and Data Protection Policy.

Use of Social Media

When using social media, staff must ensure that they comply with The Manor's Social Media Policy and Staff Behaviour Policy at all times.

Communication with pupils online

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

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