E-SAFETY (ON-LINE SAFETY) POLICY
PRESTON MANOR SCHOOL

An All-Through School

Governors' Committee Responsible: Learners Welfare	
Statutory Provision: Statutory	
Policy Author: Zalika Dale	**Review Period:** Biannual
Date reviewed: October 2023	**Next Review:** October 2025

1. Aims

Our school 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

The 4 key categories of risk

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

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, 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 scam

At Preston Manor we are hoping to gain recognition for the quality of our ICT provision through the SWGfL Online Safety Mark. We have currently secured the 'Commitment to Online Safety' Certificate and are working towards the 'Online Safety Certificate of Progress' and 'Online Safety Mark'.

2. Policy Scope

Preston Manor School believes that online safety is an essential part of safeguarding and acknowledges its duty to ensure that all students and staff are protected from potential harm online.
Preston Manor School identifies that the internet and associated devices, such as computers, tablets, mobile phones and games consoles, are an important part of everyday life.
Preston Manor School believes that students should be empowered to build resilience and to develop strategies to manage and respond to risk online. This policy applies to all staff including the governing body, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for, or provide services on behalf of the setting (collectively referred to as "staff" in this policy) as well as students, parents and carers.
This policy applies to all access to the internet and use of technology, including personal devices, or where students, staff or other individuals have been provided with setting issued devices for use off-site, such as a work laptops, tablets or mobile phones.

2.1 Legislation & Guidance

This policy is based on the Department for Education's (DfE) 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.

Preston Manor will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parent/carers of incidents of inappropriate e-safety behaviour that take place out of school.

2.2 Links with other Policies

This policy links with several other policies (but not limited to):

- Staff Code of Conduct for Employees
- Safeguarding and Child Protection Policy
- Data Protection Policy
- Discrimination and Harassment Policy
- Monitoring Policy
- Acceptable Use Policy

3. Roles and Responsibilities

The following section outlines the roles and responsibilities for e-safety of individuals and groups within the school:

3.1 The Governing Board

The governing board has overall responsibility for monitoring this policy and holding the head teacher 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 should ensure children are taught how to keep themselves and others safe, including keeping safe online.

The governing board must ensure the school 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 filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting those 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 Jonathan Bach.

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 7)

- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with SEND 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.

3.2 Headteacher and Senior Leadership Team (SLT):

- The Headteacher is responsible for ensuring the safety (including e-safety) of members of the school community
- The Headteacher / SLT will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Headteacher and at least one other member of the SLT are aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.
- Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- Provides training and advice for staff
- Liaises with ICT Support Services

3.3 The ICT Manager

The ICT manager is responsible for ensuring:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis 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 school'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
- Ensuring that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

3.4 All Staff and volunteers

Are responsible for ensuring that:

- They have an up-to-date awareness of e-safety matters and of the current school e-safety policy and practices
- They have read, understood and signed the school Staff Acceptable Use Agreement (Appendix 7)
- 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 emailing safeguarding@preston-manor.com or recording the incident on CPOMS.
- Digital communications with students should be on a professional level and only carried out using official Preston Manor systems
- E-safety issues are embedded in all aspects of the curriculum and other Preston Manor activities
- Students understand and follow Preston Manor e-safety and acceptable use policy
- Students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- They monitor ICT activity in lessons, extra-curricular and extended school activities through the use of Impero
- They are aware of e-safety issues related to the use of mobile devices and that they monitor their use and implement current Preston Manor policies with regard to these devices
- Following the correct procedures by emailing the ICT Manager and DSL, if they need to bypass the filtering and monitoring systems for educational purposes
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- In lessons where internet use is pre-planned students should be guided to sites checked as suitable for their use.
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour 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.

3.5 The designated safeguarding lead

Details of the school's DSL and deputies are set out in our child protection and safeguarding policy as well as relevant job descriptions.

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

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school child protection policy
- Ensuring that any online safety incidents are logged on CPOMs 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 school behaviour policy
- Updating and delivering staff training on online safety (appendix **4** contains a self-audit for

staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or 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.

3.6 Students

- are responsible for using Preston Manor ICT systems in accordance with the Student Acceptable Use Agreement, which they will be expected to sign before being given access to ICT systems.
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- Will be expected to know and understand Preston Manor policies on the use of mobile devices. They should also know and understand school policies on the taking / use of images and on cyber- bullying.
- Should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the E-Safety Policy covers their actions out of school, if related to their membership of the school.

3.6 Parents/Carers

Parents and carers are responsible for:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendices 1 and 2)

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

- What are the issues? – UK Safer Internet Centre
- Hot topics – Childnet International
- Parent resource sheet – Childnet International

3.7 Visitors and members of the community

- Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (see appendix 7).

4. Education

4.1 Educating students about online safety

Pupils will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise inappropriate content, contact and conduct, and know how to report concerns
- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- How to report a range of concerns

By the **end of secondary school**, pupils will know:

- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online
- Not to provide material to others that they would not want shared further and not to share personal material which is sent to them
- What to do and where to get support to report material or manage issues online
- The impact of viewing harmful content
- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence that carries severe penalties including jail
- How information and data is generated, collected, shared and used online
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours
- How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online)

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

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

4.2 Educating Parents/Carers about online safety

Parents and carers have a wide range of understanding of e-safety risks and issues, and they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line experiences

Preston Manor will seek to provide information and awareness to parents and carers through:

- Workshops, Letters, newsletters, website, VLE, Parents' evenings, Reference to External Organisations where further information can be obtained.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.

4.3 Educating Governors and Staff about online safety

Training will be offered as follows:

- A planned programme of formal e-safety training will be made available to staff.
- An audit of the e-safety training needs of all staff will be carried out regularly. It is expected that some staff will identify e-safety as a training need within the approved process.
- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand this policy and Acceptable Use Policies
- Governors should take part in e-safety training.

5. Password

Security

Introduction

Preston Manor will be responsible for ensuring that the network is as safe and secure as is reasonably possible and that:

- Users can only access data to which they have right of access
- No user should be able to access another's files, without permission (or as allowed for monitoring purposes within the school's policies).
- Access to personal data is securely controlled in line with the school's personal data policy

Responsibilities

The management of the password security policy will be the responsibility of the ICT Manager.

All users (adults and young people) will have responsibility for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.

Training / Awareness

Members of staff will be made aware of the school's password policy:

- through the school's e-safety policy and password security policy.
- through the Acceptable Use Agreement.

Students will be made aware of the school's password policy:

- in Computing lessons and/or e-safety assemblies.
- through the Acceptable Use Agreement.

All users will have clearly defined access rights to Preston Manor ICT systems. Details of the access rights available to groups of users will be recorded by the ICT Manager and will be reviewed regularly. All users will be provided with a username and password by the ICT Manager who will keep an up-to-date record of users and their usernames.

- The password should be a minimum of 8 characters long
- Authentication process should protect against brute force attacks
- Passwords shall not be displayed on screen
- Authentication shall be encrypted
- Requests for password changes should only be managed by sanctioned staff
- Only IT support staff will have access to change staff passwords
- All administrative users will use unique administrative accounts to support accountability

6. Monitoring & Filtering

The current system provides three tiers of defence. The major part of the web filtering is provided by our internet service provider, Virgin, followed by a second tier of filtering is managed by Colwyn Tech using a proprietary tool called: Smoothwall, and finally all Windows and Mac IT suites have Impero installed, which allows the classroom teacher to layer on additional white and black listings, and suspend internet access for individual students during the lesson.

Responsibilities

All users have a responsibility to report immediately to the ICT Manager (students can refer to staff who can forward the information to the ICT Manager) any infringements of the school's filtering policy of which they become aware or any sites that are accessed, which they believe should have been filtered.
Users must not attempt to use any programmes or software that might allow them to bypass the filtering / security systems in place to prevent access to such materials.

Changes to the Filtering System
Staff users may request changes to the filtering with an e-mail request to the ICT Manager and DSL. There should be strong educational reasons for changes and these changes may be for specific groups of users. The changes may be rejected for technical reasons due to the limitations of filtering systems as well as judgements about the appropriateness of materials. All changes (and requests for change) must be logged by the ICT manager.

Monitoring
The school will monitor the activities of users on the school network and on school equipment as indicated in the School E-Safety Policy and the Acceptable Use agreement. The majority of GAfE interactions are logged and can be searched using our management tool. All Windows and Mac computers have the Impero software solution that will report and record any inappropriate key-words.

The filtering policy will be reviewed in the response to the evidence provided by the audit logs of the suitability of the current provision.

7. Use of digital Photographic and Video Images

Preston Manor will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

7.1 When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.

7.2 Staff are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. These images should only be taken on school equipment the personal equipment of staff should not be used for such purposes (unless prearranged and logged with the e-safety officer).

7.3 Students must not take, use, share, publish or distribute images of others without their permission

7.4 Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images.

7.5 Students' names will not be used anywhere on a website or blog, particularly in association with photographs.

7.6 Written permission from parents or carers will be obtained before photographs of students are published on the school website.

7.7 Students' work can only be published with the permission of the student and parent/carers.

8 Social Media

8.1 Expectations

The expectations' regarding safe and responsible use of social media applies to all members of Preston Manor School.

The term social media may include (but is not limited to): blogs; wikis; social networking sites; forums; bulletin boards; online gaming; apps; video/photo sharing sites; chatrooms and instant messenger.

All members of Preston Manor School are expected to engage in social media in a positive, safe and responsible manner.

- All members of Preston Manor School are advised not to publish specific and detailed private thoughts, concerns, pictures or messages on any social media services, especially content that may be considered threatening, hurtful or defamatory to others.

We will control student and staff access to social media whilst using setting provided devices and systems on site.

- The use of social media during setting hours for personal use is not permitted.
- Inappropriate or excessive use of social media during setting hours or whilst using setting devices may result in disciplinary or legal action and/or removal of internet facilities.

Concerns regarding the online conduct of any member of Preston Manor School community on social media, should be reported to the DSL (or deputy) and will be managed in accordance with our anti-bullying, allegations against staff, behaviour and child protection policies.

8.2 Its Use in Trying to Radicalise and Recruit Young People

Preston Manor has a vital role to play in protecting pupils from the risks of extremism and radicalisation. Keeping children safe from risks posed by terrorist exploitation of social media should be approached in the same way as safeguarding children from any other online abuse.
For further information on how Social Media is being used by these groups, please see Home Office document titled 'How Social Media is Used to Encourage Travel to Syria and Iraq - Briefing Note for Schools' at following link:

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/440450/How_social_media_is_used_to_encourage_travel_to_Syria_and_Iraq.pdf

All Staff have a duty and must ensure that they alert the DSL or a member of SLT with any concerns related to a student coming into contact with any form of social media that presents a risk of radicalisation. Staff are reminded to refer to PREVENT training that they have received.

8.3 Students Personal Use of Social Media

- Safe and appropriate use of social media will be taught to students as part of an embedded and progressive education approach, via age appropriate sites and resources.
- We are aware that many popular social media sites state that they are not for children under the age of 13, therefore we will not create accounts specifically for students under this age.
- Any concerns regarding students use of social media will be dealt with in accordance with existing policies, including anti-bullying and behaviour.
    - Concerns will be shared with parents/carers as appropriate, particularly when concerning underage use of social media sites, games or tools.

- Students will be advised:
    - To consider the benefits and risks of sharing personal details on social media sites which could identify them and/or their location.
    - To only approve and invite known friends on social media sites and to deny access to others by making profiles private.
    - Not to meet any online friends without a parent/carer or other responsible adult's permission and only when a trusted adult is present.
    - To use safe passwords.
    - To use social media sites which are appropriate for their age and abilities.
    - How to block and report unwanted communications.
    - How to report concerns both within the setting and externally.

8.4 Staff Social Media Protocol

Staff members must be conscious at all times of the need to keep their personal and professional lives separate.

All individuals working on behalf of the school are bound by a legal duty of confidence and other laws to protect the confidential information they have access to during the course of their work. Disclosure of confidential information on social media is likely to be a breach of a number of laws and professional codes of conduct.

Staff who breach any of the above policies will be subject to disciplinary action up to and including termination of employment.

- The safe and responsible use of social networking, social media and personal publishing sites will be discussed with all members of staff as part of staff induction and will be revisited and communicated via regular staff training opportunities.
- Safe and professional behaviour will be outlined for all members of staff (including volunteers) as part of our code of conduct/behaviour policy as part of acceptable use policy.

Reputation

- All members of staff are advised that their online conduct on social media can have an impact on their role and reputation within the setting.
    - Civil, legal or disciplinary action may be taken if staff are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.
- All members of staff are advised to safeguard themselves and their privacy when using social media sites. Advice will be provided to staff via staff training and by sharing appropriate guidance and resources on a regular basis. This will include (but is not limited to):
    - Setting the privacy levels of their personal sites.

    - Being aware of location sharing services.
    - Opting out of public listings on social networking sites.
    - Logging out of accounts after use.
    - Keeping passwords safe and confidential.
    - Ensuring staff do not represent their personal views as that of the setting.
- Members of staff are encouraged not to identify themselves as employees of Preston Manor School on their personal social networking accounts; this is to prevent information on these sites from being linked with the setting, and to safeguard the privacy of staff members.
- All members of staff are encouraged to carefully consider the information, including text and images, they share and post online and to ensure that their social media use is compatible with their professional role and is in accordance our policies and the wider professional and legal framework.
- Information and content that staff members have access to as part of their employment, including photos and personal information about students and their family members or colleagues will not be shared or discussed on social media sites.
- Members of staff will notify the Leadership Team immediately if they consider that any content shared on social media sites conflicts with their role.

Communicating with students and parents and carers

- All members of staff are advised not to communicate with or add as 'friends' any current or past students or their family members via any personal social media sites, applications or profiles.
    - Any pre-existing relationships or exceptions that may compromise this, will be discussed with DSL (or deputies) and/or the headteacher. If ongoing contact with students is required once they have left the setting, members of staff will be expected to use existing alumni networks or use official setting provided communication tools.
    - Staff members must not have any private personal social contact through any personal social medium with any pupil, whether from Preston Manor School or any other school, unless the children or students are the member of Staff's own family members.
- Preston Manor School does not expect staff members to discontinue contact with their family members via personal social media once the school starts providing services for them. However, any information staff members obtain in the course of their employment must not be used for personal gain nor be passed on to others who may use it in such a way.
- Staff members must not have any contact with children's or students' family members through personal social media if that contact is or is likely to constitute or create a conflict of interest, call into question their objectivity or otherwise be in breach of any of the School's rules, policies and procedures.
- If Staff members wish to communicate with children or students through social media sites or to enable children or students to keep in touch with one another, they can only do so when the same standards of e-safety can be guaranteed and with the advance express written approval of the Headteacher.
- Staff members must decline 'friend requests' from children or students they receive in their personal social media accounts if they are not family members.
- On leaving Preston Manor School's service, staff members must not contact Preston Manor School's children or students by means of personal social media sites. Similarly, staff members must not contact children or students from their former schools by means of personal social media.
-

8.5 Official Use of Social Media

Staff members can only use official school sites for communicating with pupils or to enable children and students to communicate with one another. Any such use must be in strict accordance with the rules and provisions of this policy and the related policies referred to in it.

Staff must not create sites unless they are expressly authorised to do so by either the Headteacher or the Finance and Business Manager. There must be a strong pedagogical or business reason for creating official school sites to communicate with children and students or others and any member of staff wishing to create such a site must set out a proposal to the Head or the Finance and Business Manager in accordance with the provisions in this policy.

Staff members who are expressly authorised to create such a site 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.

All of our official social media channels are managed by our Marketing, Design and Communications Officer who is line managed by the Executive Head.

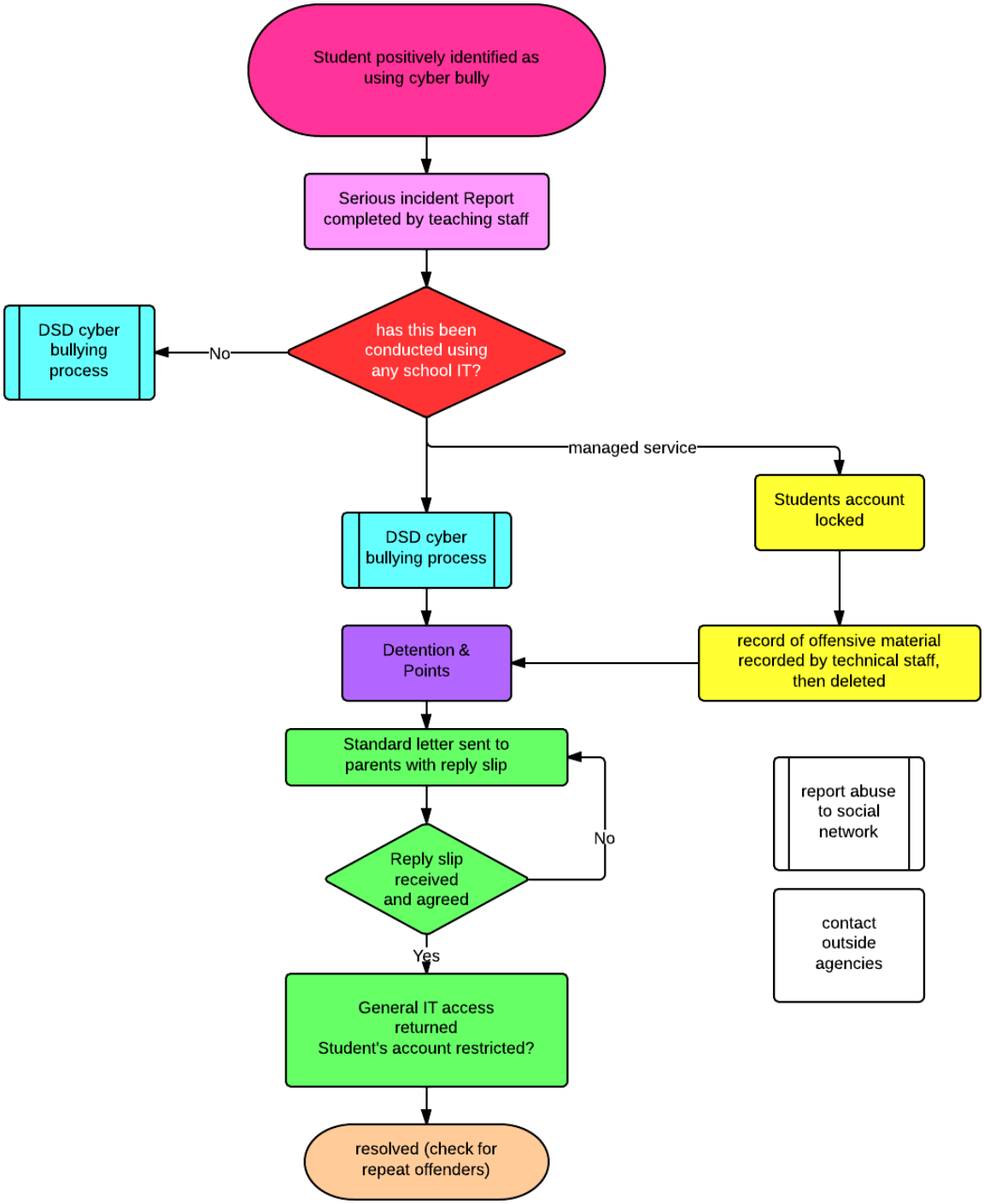
9 Cyber Bullying

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 school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be.

Cyber bullying is dealt with the same severity as other forms of bullying (refer to the bullying policy).

General Cyber Bullying Flow chart



9.1 Examining electronic devices

The headteacher, and any member of staff authorised to do so by the headteacher 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 in the school rules 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.
- 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 / headteacher / other member of the senior leadership team 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 equivalent) immediately, who will decide what to do next. The DSL 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
- Our behaviour policy

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

9.2 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 Bard.

Preston 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.

Preston Manor will treat any use of AI to bully pupils in line with our Behaviour 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.

9.3 Pupils using mobile devices in school

Pupils may bring mobile devices into school, but are not permitted to use them. They must be:

- Turned off
- Kept in their bags at all times

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, resulting in the confiscation of their device until the end of the half term.

10 Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protections Acts 1998 and 2018 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

The school will ensure that it meets the additional requirements which the General Data Protection Regulation (GDPR) places upon public bodies, and that it is fully compliant.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer personal data using encryption

- When using cloud-based storage, it is also necessary that staff ensure that only appropriate and authorised parties have shared access.

11 Staff using devices

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 are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Keeping 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 school's terms of acceptable use, as set out in appendix 3.

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 the ICT manager.

Members of Staff are strictly forbidden from sending abusive, obscene, discriminatory, racist, harassing, derogatory or defamatory messages. If such messages are received, they should not be forwarded and should be reported to a member of the Senior Leadership Team immediately.

As general guidance, Staff must not:

Send any e-mail, including re-sending and forwarding, containing sexually explicit or otherwise offensive material either internally or externally;

- Send or forward private e-mails at work which they would not want a third party to read;
- Send or forward chain mail, junk mail, either within or outside the School;
- Contribute to system congestion by unnecessarily copying or forwarding e-mails to those who do not have a real need to receive them;
- Sell or advertise using the systems.
- Agree to terms, enter into contractual commitments or make representations by e-mail unless the appropriate authority has been obtained. A name typed at the end of an e-mail is a signature in the same way as a name written in ink at the end of a letter;
- Download or e-mail text, music and other content on the internet subject to copyright protection, unless it is clear that the owner of such works allows this;
- Send messages containing any reference to other individuals or any other business that may be construed as libellous;
- Send messages from another worker's computer or under an assumed name unless specifically authorised;
- Send confidential messages via e-mail or the internet, or by other means of external communication which are known not to be secure;

11.1 Inappropriate use of equipment and systems

Misuse or abuse of our telephone or e-mail system or inappropriate use of the internet in breach of this policy will be dealt with in accordance with the School's Disciplinary Policy and Procedure.

Misuse of the internet may, in certain circumstances, constitute a criminal offence.
Any such action will be treated very seriously and may result in disciplinary action up to and including summary dismissal.

Where evidence of misuse is found the School may undertake a more detailed investigation in accordance with our Disciplinary Policy and Procedure, involving the examination and disclosure of monitoring records to those nominated to undertake the investigation and any witnesses or members of management involved in the disciplinary procedure.

If necessary such information may be handed to the police in connection with a criminal investigation.

12 Training & awareness

All staff will receive data handling awareness / data protection training and will be made aware of their responsibilities, as described in this policy through:

- Induction training for new staff
- E-safety policy in the staff handbook.
- Staff meetings / briefings / Inset as required

Appendix 1 Responding to incidents of misuse – students

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures as follows:

Students

Incidents:	Refer to class teacher / tutor	Refer to Head of Department / DSD	Refer to SLT	Refer to ICT Manager	Refer to Child Protection Officer / police	Inform parent s / carers	Monitor ring and possible restrict ions	Issue e- safety warning and sanction
Deliberate access to pornographic material		√		√	√	√	√	√
Deliberate access to images involving the sexual abuse of children		√		√	√	√	√	√
Unauthorised use of non- educational sites during lessons	√							
Unauthorised use of mobile phone / digital camera / other handheld device		√						√
Unauthorised use of social networking / instant messaging / personal email								√
Unauthorised downloading or uploading of files						√	√	√
Allowing others to access school network by sharing username and passwords						√		√
Attempting to access or accessing the school network, using another student's account						√		√
Attempting to access or accessing the school network, using the account of a member of staff		√					√	√
Corrupting or destroying the data of other users	√	√				√	√	√
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	√	√		√		√	√	√
Continued infringements of the above, following previous warnings or sanctions			√	√		√		
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		√		√			√	√
Using proxy sites or other means to subvert the school's filtering system							√	√
Accidentally accessing offensive or pornographic material and failing to report the incident						√		
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protections Acts 1998 and 2018						√	√	√

Appendix 2 Responding to incidents of misuse – Staff

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures as follows:

Staff

Incidents:	Refer to line manager	Refer to SLT	Refer to child protection officer / police	Refer to e- safety officer	Watch list	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	√			√	√	√	potentially	potentially
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email	√			√	√	√	potentially	potentially
Unauthorised downloading or uploading of files	√			√	√	√	potentially	potentially
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	√			√		√	potentially	potentially
Careless use of personal data eg holding or transferring data in an insecure manner	√			√	√			
Deliberate actions to breach data protection or network security rules	√	√		√	√	potentially	potentially	potentially
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	√	√		√	√	√		
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	√	√		√	√		potentially	potentially
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students	√	√	√	√	√	√	potentially	potentially
Actions which could compromise the staff member's professional standing	√	√			√		potentially	
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	√	√			√		potentially	

Using proxy sites or other means to subvert the school's filtering system	√	√		√	√		potentially	potentially
Accidentally accessing offensive or pornographic material and failing to report the incident	√		√	√			potentially	potentially
Deliberately accessing or trying to access offensive or pornographic material		√	√	√	√		potentially	potentially
Breaching copyright or licensing regulations	√	√		√	√		potentially	potentially
Continued infringements of the above, following previous warnings or sanctions		√	√				√	√

Appendix 3 Student Acceptable Use Policy Agreement

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS	
Name of pupil:	
I will read and follow the rules in the acceptable use agreement policy. **When I use the school's ICT systems (like computers) and get onto the internet in school I will:** • Always use the school's ICT systems and the internet responsibly and for educational purposes only • Only use them when a teacher is present, or with a teacher's permission • Keep my usernames and passwords safe and not share these with others • Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer • Tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others • Always log off or shut down a computer when I've finished working on it **I will not:** • Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity • Open any attachments in emails, or follow any links in emails, without first checking with a teacher • Use any inappropriate language when communicating online, including in emails • Create, link to or post any material that is pornographic, offensive, obscene or otherwise inappropriate • Log in to the school's network using someone else's details • Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision **If I bring a personal mobile phone or other personal electronic device into school:** • I will keep it in my bag and turned off at all times **I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.**	
Signed (pupil):	• **Signed (pupil):**
Parent/carer's agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.	
Signed (parent/carer):	**Signed (parent/carer):**

Think before you click

S	I will only use the Internet and email with an adult
A	I will only click on icons and links when I know they are safe
F	I will only send friendly and polite messages
E	If I see something I don't like on a screen, I will always tell an adult

My Name:

My Signature:

All

Appendix 4 Staff Acceptable Use Policy Agreement

This Acceptable Use Policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that Preston Manor ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of ICT in their everyday work.

Preston Manor will try to ensure that staff and volunteers will have good access to ICT to enhance their work, to enhance learning opportunities for students learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that students receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed e-safety in my work with young people.

For my professional and personal safety, I understand that:

- that Preston Manor will monitor my use of the ICT systems, email and other digital communications.
- that the rules summarised in this agreement and detailed in the e-safety policy also apply to use of Preston Manor ICT systems (eg laptops, email, Google Classroom, VLE etc) out of school.
- that Preston Manor ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

My communications and actions when using school ICT systems will be professional. I will:

- not access, copy, remove or otherwise alter any other user's files, without their express permission.
- communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (eg on Preston Manor website / VLE) it will not be possible to identify by name, or other personal information, those who are featured.
- only use chat and social networking sites in school in accordance with this policy.
- only communicate with students and parents / carers using official Preston Manor systems. Any such communication will be professional in tone and manner.
- not engage in any on-line activity that may compromise my professional responsibilities.

Preston Manor has the responsibility to provide safe and secure access to technologies and ensure the smooth running of the schools. When I use my personal handheld / mobile devices (tablets / laptops / mobile phones / etc) in school, I will:

- follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by Preston Manor about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
- ensure that my data is regularly backed up, in accordance with relevant Preston Manor policies.
- not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others.
- not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies.
- not disable or cause any damage to Preston Manor equipment, or the equipment belonging to others.
- only transport, hold, disclose or share personal information about myself or others, as outlined in the Personal Data Policy.
- immediately report to the ICT Support Department any damage or faults involving equipment or software, however this may have happened.

I understand that data protection policy requires that any staff or student data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by Preston Manor policy to disclose such information to an appropriate authority.

When using the internet in my professional capacity or for Preston Manor sanctioned personal use. I will:

- ensure that I have permission to use the original work of others in my own work
- not download or distribute copies (including music and videos) where work is protected by copyright.

I understand that I am responsible for my actions in and out of school, and that:

- this Acceptable Use Policy applies not only to my work and use of Preston Manor ICT equipment in school, but also applies to my use of Preston Manor ICT systems and equipment out of school and my use of personal equipment in school or in situations related to my employment by the Federation.
- if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and / or the Local Authority and in the event of illegal activities the involvement of the police.
- In the event of any breach, or potential breach of Data privacy, I will immediately report this to the Data Protection Officer (Ms. Natalie Kampta) and a member of the Senior Leadership Team.

I have read and understand the above and agree to use Preston Manor ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff / Volunteer Name

Signed Date

Appendix 5 Parent/Carer Acceptable Use Guidance

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Guidance is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that parents and carers are aware of the importance of e-safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

The school will try to ensure that students will have good access to ICT to enhance their learning and will, in return, expect the students to agree to be responsible users. A copy of the Student / Pupil Acceptable Use Policy is attached to this guidance, so that parents / carers will be aware of the school expectations of the young people in their care.

Please ensure that your child has signed an Acceptable Use Agreement.

Throughout their schooling at Preston Manor they will receive, e-safety education to help them understand the importance of safe use of ICT – both in and out of school.

The school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems. The school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies. Your Child's activity on the ICT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

Please encourage your child to adopt safe use of the internet and digital technologies at home and feel free to contact the school if you have concerns over your child's e-safety.

Appendix 6 Permission Form for use of digital/video images

The use of digital / video images plays an important part in learning activities. Students and members of staff may use digital cameras to record evidence of activities in lessons and out of school. These images may then be used in presentations in subsequent lessons.

Images may also be used to celebrate success through their publication in newsletters, on the school website and occasionally in the public media.

The school will comply with the Data Protections Acts 1998 and 2018 and request parent/carers permission before taking images of members of the school.

We will also ensure that when images are published that the young people cannot be identified by the use of their names.

Parent/Carers are requested to sign the permission form below to allow the school to take and use images of their children.

Parent/Carer's

Name Student

Name

As the parent/carer of the above student, I agree to the school taking and using digital / video images of my child. I understand that the images will only be used to support learning activities or in publicity that reasonably celebrates success and promotes the work of the school.

I agree that if I take digital or video images at school events which include images of children, other than my own, I will abide by these guidelines in my use of these images.

Signed Date

Appendix 7: online safety training needs – self-audit for staff

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/volunteer:	**Date**:
Question	**Yes/No (add comments if necessary)**
Do you know the name of the person who has lead responsibility for online safety in school?	
Are you aware of the ways pupils can abuse their peers online?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents/carers?	
Are you familiar with the filtering and monitoring systems on the school's devices and networks?	
Do you understand your role and responsibilities in relation to filtering and monitoring?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	

Appendix 8 Responding to Student Radicalisation

Student radicalisation often occurs via electronic media. The school appreciates its key role in the Prevent strategy. When staff identify that a student demonstrates significant indications that they are potentially being radicalised, they will inform the Child Protection Officer.
The school's filtering system reduced access to sites that support terrorism. The monitoring system also tracks key words associated with radicalisation, for example, anti-Semitic terms.