Perryfields Enterprise Academy Trust

Online Safety Policy

Adapted From:	Adapted from TheKey
Approved By:	P.E.A.T Board
Reviewed:	October 2023
Approved Date:	7th December 2023
Review:	Annually - or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place.
Next Review Date:	October 2024
Communicated to Staff	By: Email Date: 13th December 2023
Published on:	PEAT & PJS website

SUMMARY OF CHANGES – OCTOBER 2023	
Section	**Detail**
Our Commitment pg.3	Added fourth area of risk - Commerce
Legislation and Guidance	Updated to reflect KCSIE 2023 wording.
Local Governing Body Governors	Additional wording to emphasise the role and responsibilities of the governing board in relation to online safety, particularly around maintaining filtering and monitoring systems and staff training, to reflect changes in Keeping Children Safe in Education (KCSIE) 2023.
Headteacher/Head of School and Senior Leaders	Additional wording re Headteachers responsibility for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.
Online Safety Coordinator in P.E.A.T Schools	Additional wording re supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school.
Online Safety Coordinator in P.E.A.T Schools	Additional wording re adapting teaching for pupils with SEND or those vulnerable students.
Online Safety Coordinator in P.E.A.T Schools	Added the responsibility that the Online Safety Coordinator holds for the school filtering and monitoring systems to reflect changes in Keeping Children Safe in Education (KCSIE) 2023.
Designated Child Protection Co-Ordinators	Additional wording – *"This list is not intended to be exhaustive."*
Network Manager	Additional wording – *"blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files"*
All staff and volunteers in P.E.A.T Schools	Section title changed from Teaching and support staff in P.E.A.T Schools
All staff and volunteers in P.E.A.T Schools	Updated wording to include all staff. Additional wording re filtering and monitoring systems, cyber bullying, concerns re; sexual violence or harassment (both online and offline). Additional wording – *"This list is not intended to be exhaustive."*
Parents/Carers	Additional wording re parent/carer expectations.
Policy statements - Education Pupils	Additional bullet points under heading; Pupils in Key Stage 2 will be taught to and By the end of primary school, pupils will know
Policy statements - Education Parents/carers	Additional wording about where/who parents/carers should reports concerns to.
Appendix 1 1. Cyberbullying	Updated the cyber-bullying section to include a section about artificial intelligence (AI), which includes a clause related to the potential misuse of generative AI, such as ChatGPT and Google Bard in relation to 'deepfakes'.

Perryfields Enterprise Academy Trust
Online Safety Policy

Development / Monitoring / Review of this Policy

This Online Safety Policy has been developed by a working group made up of:

- *Executive Headteacher*
- *Online Safety Co-ordinator*
- *Staff*
- *The Directors of Perryfields Enterprise Academy Trust*

Schedule for Development / Monitoring / Review

The implementation of this Online Safety Policy will be monitored by the:	Online Safety Co-ordinator Headteacher
Monitoring will take place at regular intervals:	Annually or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be: October 2022
The Local Governing Body will receive a report on the implementation of the Online Safety Policy (which will include anonymous details of online safety incidents):	Annually
The P.E.A.T. Board will receive a report from the LGBs annually	Annually
Should serious online safety incidents take place, the following external agencies may need to be informed:	Essex Social Services Police

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring data for network activity
- Feedback from pupils and staff

Scope of the Policy

This policy applies to all members of the P.E.A.T. community (including staff, pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of P.E.A.T. schools.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the *school* site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other online safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

P.E.A.T schools will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate online safety behaviour that take place out of school.

Our Commitment

The P.E.A.T is committed to ensure safer lives and even more remarkable learning for all children and young people. As we increasingly work, learn and teach online, it is essential that children are safeguarded from potentially harmful and appropriate online material.

The use of technology has become a significant component of many safeguarding issues. Child sexual exploitation; radicalisation; sexual predation: often proves the platform that facilitates harm Please see **Appendix 1: Online safeguarding issues**.

The breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk;

a) **Content:** being exposed to illegal, inappropriate or harmful material; for example pornography, fake news, racist or radical and extremist views;
b) **Contact:** being subjected to harmful online interaction with other users; for example commercial advertising as well as adults posing as children or young adults; and
c) **Conduct:** personal online behaviour that increases the likelihood of, or causes, harm; for example making, sending and receiving explicit images, or online bullying.
d) **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

Accordingly, we have appropriate internet filtering and this is regularly monitored within the school setting. The welfare and safety of each individual child is paramount and therefore we are committed to providing a safe online learning environment by:

a) Ensuring robust processes are in place to ensure the online safety of pupils, staff, volunteers and governors.
b) Delivering an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology.
c) Establishing clear mechanisms to identify, intervene and escalate an incident where appropriate.

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
- 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.

We also follow the online safety guidance as recommended within Keeping Children Safe in Education within our delivery of remote education, virtual lessons and live streaming. This includes a range of resources and guidance for Perryfields staff, parents and carers, pupils. Please see **Appendix 2: Useful links and resources for staff, pupils and parents**

This policy complies with our funding agreement and articles of association.

Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within P.E.A.T **schools**: The use of the term regular will mean at least once a term or more often if required.

P.E.A.T. Directors:

P.E.A.T. Directors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy.

Local Governing Body Governors:

The LGB Governors are responsible for the adoption and monitoring of the Online Safety Policy and for informing the PEAT Board of the effectiveness of the policy. This will be carried out by LGB Governors receiving regular information about online safety incidents and monitoring reports. A member of the LGB Governing Body will take on the role of Online Safety Governor. The role of the Online Safety Governor will include:

- regular meetings with the Online Safety Co-ordinator
- regular monitoring of online safety incident logs
- reporting to the LGB and, if required, the PEAT Board

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.

All governors will:

a) Ensure that they have read and understood this policy.
b) Sign to confirm they agree and adhere to the terms on acceptable use as detailed in the ICT Acceptable Use Policy.
c) Governors and proprietors should ensure that staff undergo regularly updated safeguarding training and that online safety training is integrated, aligned and considered as part of the overarching safeguarding approach.

Headteacher/Head of School and Senior Leaders:

- P.E.AT Headteachers are responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.
- P.E.A.T Headteachers have a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the Online Safety Co-ordinator.
- P.E.A.T Headteachers and another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.
- P.E.A.T Headteachers are responsible for ensuring that the Online Safety Coordinator and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.

- P.E.A.T Headteachers will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- P.E.A.T Senior Leadership Teams will receive regular monitoring reports from the Online Safety Co-ordinator.

Online Safety Coordinator in P.E.A.T. schools:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies and documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place
- provides training and advice for staff
- liaises with the P.E.A.T. Board as necessary
- liaises with school technical staff
- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments
- meets regularly with Online Safety LGB Governor to discuss current issues, review incident logs and filtering / change control logs
- reports regularly to Senior Leadership Team
- reports annually to the Local Governing Body
- ensures that they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- 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

Network Manager:

is responsible for ensuring:

- that P.E.A.T schools' technical infrastructure is secure and is not open to misuse or malicious attack
- that P.E.A.T schools meets required online safety technical requirements
- that users may only access the networks and devices through a properly enforced password protection policy
- the filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- that the use of the network / internet / DB Primary / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Online Safety Coordinator for investigation
- that monitoring software / systems are implemented and updated as agreed in school policies

- that P.E.A.T school's Online Safety Co-ordinator is updated with regular reports on the school systems
- blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

All staff and volunteers in P.E.A.T. Schools

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 P.E.A.T acceptable use of the ICT agreement
- 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 to the school's Online Safety Coordinator.
- following the correct procedures by approaching the school's Online Safety Coordinator 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 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'
- they have an up to date awareness of online safety matters and of the current school online safety policy and practices
- they have read, understood and signed the school's Code of Conduct as set out in the staff handbook
- they report any suspected misuse or problem to the Online Safety Coordinator for investigation
- all digital communications with pupils / parents / carers should be on a professional level and only carried out using official school systems
- online safety issues are embedded in all aspects of the curriculum and other activities
- pupils understand and follow the online safety and acceptable use policies
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- in lessons where internet use is pre-planned, pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
- ensure children have secure access to remote learning where required (see Remote Learning Policy).

This list is not intended to be exhaustive.

Designated Child Protection Co-ordinators

Details of Perryfields' designated safeguarding lead (DSL) are set out in our Safeguarding and Child Protection policy. The DSL takes lead responsibility for online safety in school, in particular:

a) Ensuring that staff understand this policy and that it is being implemented consistently throughout Perryfields
b) Working with the appropriate staff members, as necessary, to address any online safety issues or incidents
c) Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
d) Ensuring that any incidents of cyberbullying are logged and dealt with appropriately in line with the school behaviour policy
e) Updating and delivering staff training on online safety
f) Liaising with other agencies and/or external services if necessary
g) Providing regular reports on online safety in school to the headteacher and/or governing board
h) Monitoring CPOMS incident reports and, where designated to do so and taking appropriate action
i) Ensuring staff involved in the delivery of online learning adhere to the Online Learning policy

This list is not intended to be exhaustive.

Pupils

- are responsible for using the school digital technology systems in accordance with the Responsible Use of the Internet and DB Primary
- 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 policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying.
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's online safety Policy covers their actions out of school, if related to their membership of the school

Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet and mobile devices in an appropriate way. P.E.A.T schools will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about national / local online safety campaigns / literature. Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website and online pupil records
- their children's personal devices in the school (where this is allowed)

Parents/carers are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy

Policy Statements

Education – pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety is therefore an essential part of P.E.A.T school's online safety provision. Children and young people need the help and support of their school to recognise and avoid online safety risks and build their resilience.

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned online safety curriculum should be provided as part of Computing / PSHE / other lessons (including Relationships Education, September 2020) and should be regularly revisited
- Key online safety messages should be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities
- Pupils should be taught in all lessons to be critically aware of the materials / content they access online and be guided to validate the accuracy of information.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils should be helped to understand the need for the Responsible Use of the Internet and DB Primary and encouraged to adopt safe and responsible use both within and outside school
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices
- In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

Pupils in **Key Stage (KS) 2** 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

By the **end of primary school**, 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

Education – parents / carers

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring and regulation of the children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

P.E.A.T schools will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters, newsletters, website
- High profile events and campaigns
- Reference to the relevant web sites and publications

If parents/carers 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.

Education – The Wider Community

- P.E.A.T school website will provide online safety information for the wider community
- Liaising with feeder schools in ensuring co-ordinated advice to parents and carers

Education & Training – Staff / Volunteers

It is essential that all P.E.A.T. staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced.
- All new staff should MUST receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and Code of Conduct.
- The Online Safety Coordinator will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.
- This Online Safety Policy and its updates will be presented to and discussed by staff in staff meetings and INSET days.
- The Online Safety Coordinator will provide advice, guidance and training to individuals as required.

Training – P.E.A.T. Directors and LGB Governors

P.E.A.T. Directors and LGB Governors should take part in online safety training and awareness sessions, with particular importance for those who are members of any group involved in technology / online safety / health and safety / child protection. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority / National Governors Association / or other relevant organisation (eg SWGfL).
- Participation in school training / information sessions for staff or parents.

Technical – infrastructure / equipment, filtering and monitoring

P.E.A.T schools will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. They will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities:

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements
- There will be regular reviews and audits of the safety and security of school academy technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school technical systems and devices.
- All users will be provided with a username and secure password by the Online Safety Co-ordinator who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password.
- The administrator passwords for the school ICT system, used by the Network Manager (or other person) must also be available to the Headteacher and other nominated staff.
- The school is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations.
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider.
- Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes.
- An appropriate system is in place for users to report any actual / potential technical incident / security breach to the relevant person.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- An agreed procedure is in place for the provision of temporary access of “guests” (eg trainee teachers, supply teachers, visitors) onto the school systems.
- The Code of Conduct sets out the extent of personal use that users are allowed on school devices that may be used out of school.
- An agreed policy is in place regarding the use of removable media (eg memory sticks / CDs / DVDs).

Bring Your Own Device (BYOD)

The educational opportunities offered by mobile technologies are being expanded as a wide range of devices, software and online services become available for teaching and learning, within and beyond the classroom. This has led to the exploration by schools of users bringing their own technologies in order to provide a greater freedom of choice and usability. However, there are a number of online safety considerations for BYOD that need to be reviewed prior to implementing such a policy. Use of BYOD should not introduce vulnerabilities into existing secure environments. Considerations will need to include; levels of secure access, filtering, data protection, storage and transfer of data, mobile device management systems, training, support, acceptable use, auditing and monitoring.

- The school has a set of clear expectations and responsibilities for all users

- The school adheres to the Data Protection Act principles
- All users are provided with and accept the Code of Conduct
- All network systems are secure and access for users is differentiated
- Where possible these devices will be covered by the school's normal filtering systems, while being used on the premises
- All users will use their username and password and keep this safe
- Mandatory training is undertaken for all staff
- Pupils receive training and guidance on the use of personal devices
- Regular audits and monitoring of usage will take place to ensure compliance

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students / pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils 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 eg on social networking sites.
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other pupils in the digital / video images.
- Staff and volunteers 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. Those images should only be taken on school equipment. The personal equipment of staff can be used at the school's discretion for such purposes if school equipment is unavailable but digital / video images must be permanently removed immediately after use.
- Care should be taken when taking digital / video images that students / pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include students / pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of students / pupils are published on the school website
- Pupil's work can only be published with the permission of the student / pupil and parents or carers.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 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.

All matters regarding data protection are covered in the school's Data Protection Policies.

Social Media - Protecting Professional Identity

All schools and academies have a duty of care to provide a safe learning environment for pupils and staff. Schools/academies and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

P.E.A.T schools provide the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through limiting access to personal information:

- Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

P.E.A.T. School staff should ensure that:

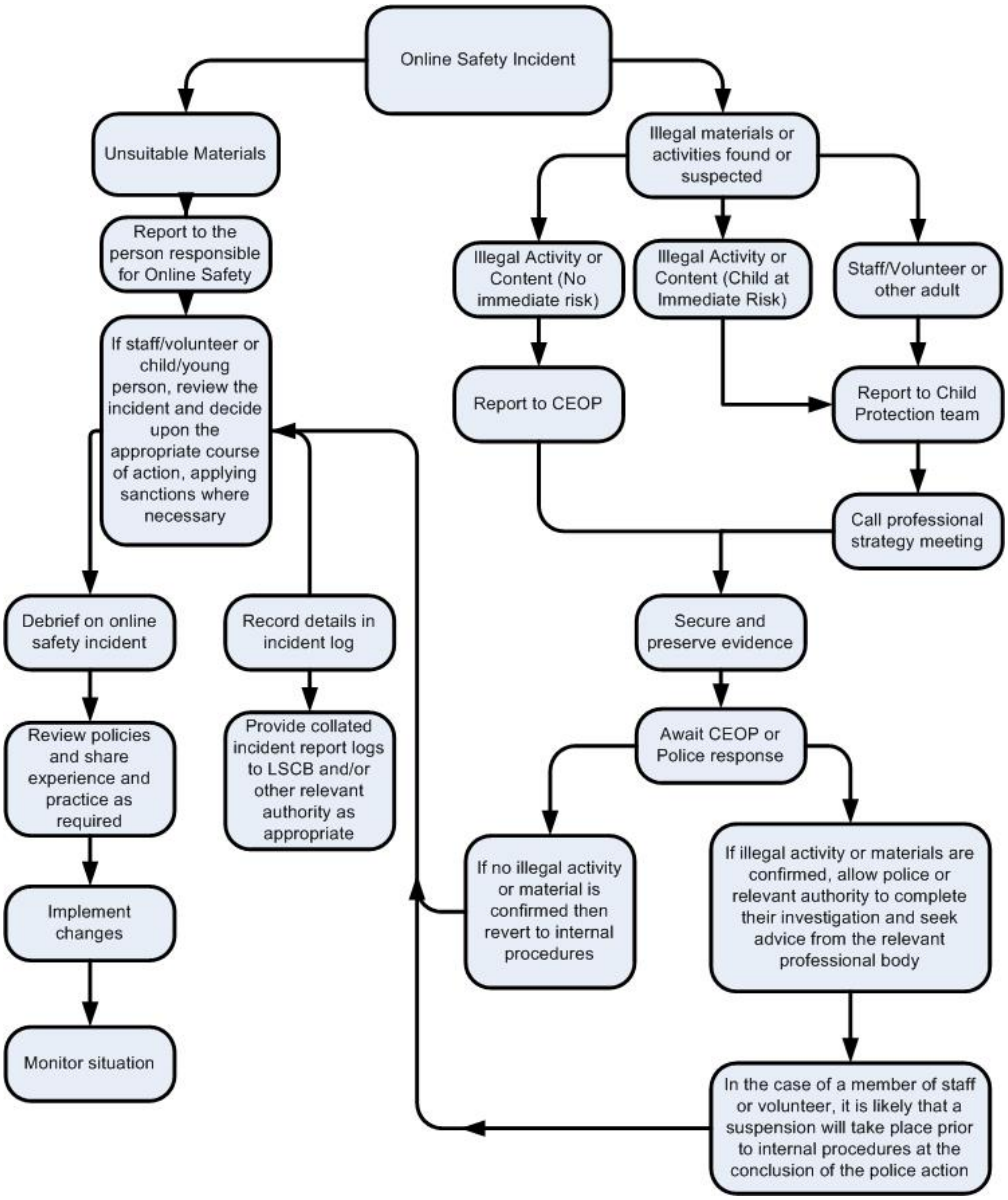
- No reference should be made in social media to students / pupils, parents / carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see "User Actions" above).

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right-hand side of the Flowchart (below and appendix) for responding to Online safety incidents and report immediately to the police.



Other Incidents

It is hoped that all members of the P.E.A.T. community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff / volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the url of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)

- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:

    - Internal response or discipline procedures
    - Involvement by national / local organisation (as relevant).
    - Police involvement and/or action

- If content being reviewed includes images of Child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:

    - incidents of 'grooming' behaviour
    - the sending of obscene materials to a child
    - adult material which potentially breaches the Obscene Publications Act
    - criminally racist material
    - other criminal conduct, activity or materials

- Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the group for evidence and reference purposes.

School Actions & Sanctions

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.

Appendix 1: Online safeguarding issues

1. Cyberbullying:

Cyberbullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bulling, it is repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school's Behaviour policy.)

Cyberbullying can also be a form of peer on peer abuse through sexual harassment that happens through the use of technology online. For example, young people may be persuaded or forced to share sexually explicit images of themselves, have sexual conversations by text, or take part in sexual activities using a webcam.

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.

P.E.A.T 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.

P.E.A.T School's will treat any use of AI to bully pupils in line with our [anti-bullying/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/trust.

3. Preventing and addressing cyberbullying

To help prevent cyberbullying, 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.

Perryfields will actively discuss cyberbullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Teachers will discuss cyber-bullying with their classes when appropriate, and the issue will be addressed in assemblies.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyberbullying. This includes personal, social, health and economic (PSHE) education, and other subjects 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.

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

In relation to a specific incident of cyberbullying, Perryfields will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

4. Preventing radicalisation

Children are vulnerable to extremist ideology and radicalisation. Similar to protecting children from other forms of harms and abuse, protecting children from this risk is part of our safeguarding approach**.**

5. Extremism

Extremism goes beyond terrorism and is defined as the vocal or active opposition to our fundamental values, including the rule of law, individual liberty and the mutual respect and tolerance of different faiths and beliefs.

This also includes calling for the death of members of the armed forces (As defined in the Government's Counter Extremism Strategy)

Extremists often target the vulnerable - including the young- by seeking to sow divisions between communities on the basis of race, faith or denomination; justifying discrimination towards women and girls; seeking to persuade others that minorities are inferior; or arguing against the primacy of democracy and the rule of law in our society.

6. Radicalisation

Radicalisation refers to the process by which a person comes to support terrorism and extremist ideologies associated with terrorist groups.

There is no single way of identifying whether a child is likely to be susceptible to an extremist ideology. Background factors combined with specific influences such as family and friends may contribute to a child's vulnerability.

Similarly, radicalisation can occur through many different methods (such as social media) and settings (such as the internet). However, it is possible to protect vulnerable people from extremist ideology and intervene to prevent those at risk of radicalisation being radicalised.

As with other safeguarding risks, staff should be alert to changes in children's behaviour which could indicate that they may be in need of help or protection. Staff should use their judgement in identifying children who might be at risk of radicalisation and act proportionately which may include the designated safeguarding lead (or deputy) making a referral to the Channel programme.

7. The Prevent Duty

All schools and colleges are subject to a duty under section 26 of the CounterTerrorism and Security Act 2015 (the CTSA 2015), in the exercise of their functions, to have "due regard to the need to prevent people from being drawn into terrorism".

This duty is known as the **Prevent** duty. The Prevent duty should be seen as part of schools' and colleges' wider safeguarding obligations. Designated safeguarding leads and other senior leaders should familiarise themselves with the Revised Prevent duty guidance: for England and Wales, especially paragraphs 57-76 which are specifically concerned with schools (and also covers childcare). The guidance is set out in terms of four general themes: Risk assessment, working in partnership, staff training, and IT policies. Schools have a duty to prevent children from being drawn into terrorism. The DSL will undertake Prevent awareness training and make sure that staff have access to appropriate training to equip them to identify children at risk.

We will assess the risk of children in our school being drawn into terrorism. This assessment will be based on an understanding of the potential risk in our local area, in collaboration with our local safeguarding children board and local police force.

We will ensure that suitable internet filtering is in place and equip all pupils to stay safe online at school and at home.

There is no single way of identifying an individual who is likely to be susceptible to an extremist ideology. Radicalisation can occur quickly or over a long period. Staff will be alert to changes in pupils' behaviour to ensure early identification of risk.

The government website Educate Against Hate and charity NSPCC say that signs that a pupil is being radicalised can include:

1. Refusal to engage with, or becoming abusive to, peers who are different from themselves
2. Becoming susceptible to conspiracy theories and feelings of Persecution
3. Changes in friendship groups and appearance
4. Rejecting activities they used to enjoy
5. Converting to a new religion
6. Isolating themselves from family and friends
7. Talking as if from a scripted speech
8. An unwillingness or inability to discuss their views
9. A sudden disrespectful attitude towards others
10. Increased levels of anger
11. Increased secretiveness, especially around internet use
12. Expressions of sympathy for extremist ideologies and groups, or justification of their actions
13. Possessing extremist literature
14. Being in contact with extremist recruiters and joining, or seeking to join, extremist organisations

8. Children who are at risk of radicalisation may have a low self-esteem or be victims of bullying or discrimination.

It is important to note that these signs can also be part of normal developing behaviour – staff should have confidence in their instincts and seek advice if something feels wrong.

If staff are concerned about a pupil, they will follow our procedures set out in this policy, including discussing their concerns with the DSL. Staff should always take action if they are worried.

9. Additional support

The department has published advice for schools on the Prevent duty. to complement the Prevent guidance and signposts other sources of advice and support. Prevent duty guidance: for further education institutions in England and Wales that applies to colleges. Educate Against Hate, a website launched by Her Majesty's Government has been developed to support and equip school and college leaders, teachers, and parents with information, tools and resources (including on the promotion of fundamental British values) to help recognise and address extremism and radicalisation in young people. The platform provides information on and access to training resources for teachers, staff and school and college leaders, some of which are free such as Prevent e-learning, via the Prevent Training catalogue.

10. Channel

Channel is a programme which focuses on providing support at an early stage to people who are identified as being vulnerable to being drawn into terrorism. It provides a mechanism for schools to make referrals if they are concerned that an individual might be vulnerable to radicalisation.

An individual's engagement with the programme is entirely voluntary at all stages. Guidance on Channel is available at: Channel guidance, and a Channel awareness e-learning programme is

available for staff at: Channel General Awareness.

The school or college's Designated Safeguarding Lead (and any deputies) should be aware of local procedures for making a Channel referral.

As a Channel partner, the school or college may be asked to attend a Channel panel to discuss the individual referred to determine whether they are vulnerable to being drawn into terrorism and consider the appropriate support required.

11. Contextual factors

Safeguarding incidents and/or behaviours can be associated with factors outside Perryfields/ or can occur between children outside the school or college. This can involve violent, humiliating and degrading sexual assaults, but does not always involve physical contact and can happen through the use of technology online. For example, young people may be persuaded or forced to share sexually explicit images of themselves, have sexual conversations by text, or take part in sexual activities using a webcam.

All staff, but especially the designated safeguarding lead (or deputy) should be considering the context within which such incidents and/or behaviours occur. This is known as contextual safeguarding, which simply means assessments of children should consider whether wider environmental factors are present in a child's life that are a threat to their safety and/or welfare.

Children's social care assessments should consider such factors so it is important that schools and colleges provide as much information as possible as part of the referral process. This will allow any assessment to consider all the available evidence and the full context of any abuse.

Appendix 2: Useful links and resources for staff, pupils and parents

Opportunities to teach online safety to pupils:

- Be Internet Legends developed by Parent Zone and Google is a free internet safety curriculum with PSHE accredited lesson plans and teaching resources for Key Stage 2 pupils
- Disrespectnobody is Home Office advice and includes resources on healthy relationships, including sexting and pornography
- Education for a connected world framework from the UK Council for Internet Safety supports the development of the curriculum and is of particular relevance to RSHE education and Computing. It is designed, however, to be usable across the curriculum and beyond (covering early years through to age 18) and to be central to a whole school or college approach to safeguarding and online safety.
- PSHE association provides guidance to schools on developing their PSHE curriculum
- Teaching online safety in school is departmental guidance outlining how schools can ensure their pupils understand how to stay safe and behave online as part of existing curriculum requirements
- Thinkuknow is the National Crime Agency/CEOPs education programme with age specific resources
- Sexting: responding to incidents and safeguarding children - UK Council for Internet Safety. UK Safer Internet Centre has developed further guidance and resources that can help with the teaching of the online safety component of the Computing Curriculum.

Advice for governing bodies/proprietors and senior leaders:

- Childnet provide guidance for schools on cyberbullying
- Educateagainsthate provides practical advice and support on protecting children from extremism and radicalisation
- London Grid for Learning provides advice on all aspects of a school or college's online safety arrangements
- NSPCC provides advice on all aspects of a school or college's online safety arrangements
- Searching screening and confiscation is departmental advice for schools on searching children and confiscating items such as mobile phones
- South West Grid for Learning provides advice on all aspects of a school or college's online safety arrangements
- Use of social media for online radicalisation - A briefing note for schools on how social media is used to encourage travel to Syria and Iraq
- UK Council for Internet Safety have provided advice on sexting-in-schools-andcolleges and using-external-visitors-to-support-online-safety-education

Remote education, virtual lessons and live streaming:

- Case studies on remote education practice are available for schools to learn from each other
- Departmental guidance on safeguarding and remote education including planning remote education strategies and teaching remotely
- London Grid for Learning guidance, including platform specific advice
- National cyber security centre guidance on choosing, configuring and deploying video conferencing
- National cyber security centre guidance on how to set up and use video conferencing
- UK Safer Internet Centre guidance on safe remote learning

Support for children:

- Childline for free and confidential advice
- UK Safer Internet Centre to report and remove harmful online content
- CEOP for advice on making a report about online abuse

Parental support:

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

- Childnet International offers a toolkit to support parents and carers of children of any age to start discussions about their online life, to set boundaries around online behaviour and technology use, and to find out where to get more help and support
- Commonsensemedia provide independent reviews, age ratings, & other information about all types of media for children and their parents
- Government advice about protecting children from specific online harms such as child sexual abuse, sexting, and cyberbullying
- Government advice about security and privacy settings, blocking unsuitable content, and parental controls
- Internet Matters provide age-specific online safety checklists, guides on how to set parental controls on a range of devices, and a host of practical tips to help children get the most out of their digital world
- Let's Talk About It provides advice for parents and carers to keep children safe from online radicalisation
- London Grid for Learning provides support for parents and carers to keep their children safe online, including tips to keep primary aged children safe online
- Lucy Faithfull Foundation StopItNow resource can be used by parents and carers who are concerned about someone's behaviour, including children who may be displaying concerning sexual behaviour (not just about online)
- National Crime Agency/CEOP Thinkuknow provides support for parents and carers to keep their children safe online
- Net-aware provides support for parents and carers from the NSPCC and O2, including a guide to social networks, apps and games
- Parentzone provides help for parents and carers on how to keep their children safe online
- Parent info from Parentzone and the National Crime Agency provides support and guidance for parents from leading experts and organisations
- UK Safer Internet Centre provide tips, advice, guides and other resources to help