Perryfields Enterprise Academy Trust

Online Safety Policy

Adapted From:	ECC Policy
Approved By:	P.E.A.T Board
Reviewed:	November 2020
Approved Date:	9th December 2020
Accepted by LGB:	9th December 2020
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:	December 2021
Communicated to Staff	By: Email Date: 6th January 2021
Published on:	PEAT & PJS website

SUMMARY OF CHANGES – NOVEMBER 2020	
Page	**Detail**
4	Additional bullet point added “to ensure children have access to remote learning when required”.

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 2021
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 (see appendix for template policy). 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.

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:

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

Headteacher/Head of School and Senior Leaders:

- 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:

- 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

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

Teaching and Support Staff in P.E.A.T. Schools

are responsible for ensuring that:

- 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).

Designated Child Protection Co-ordinators

Must be trained in online safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying

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)

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.

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

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:

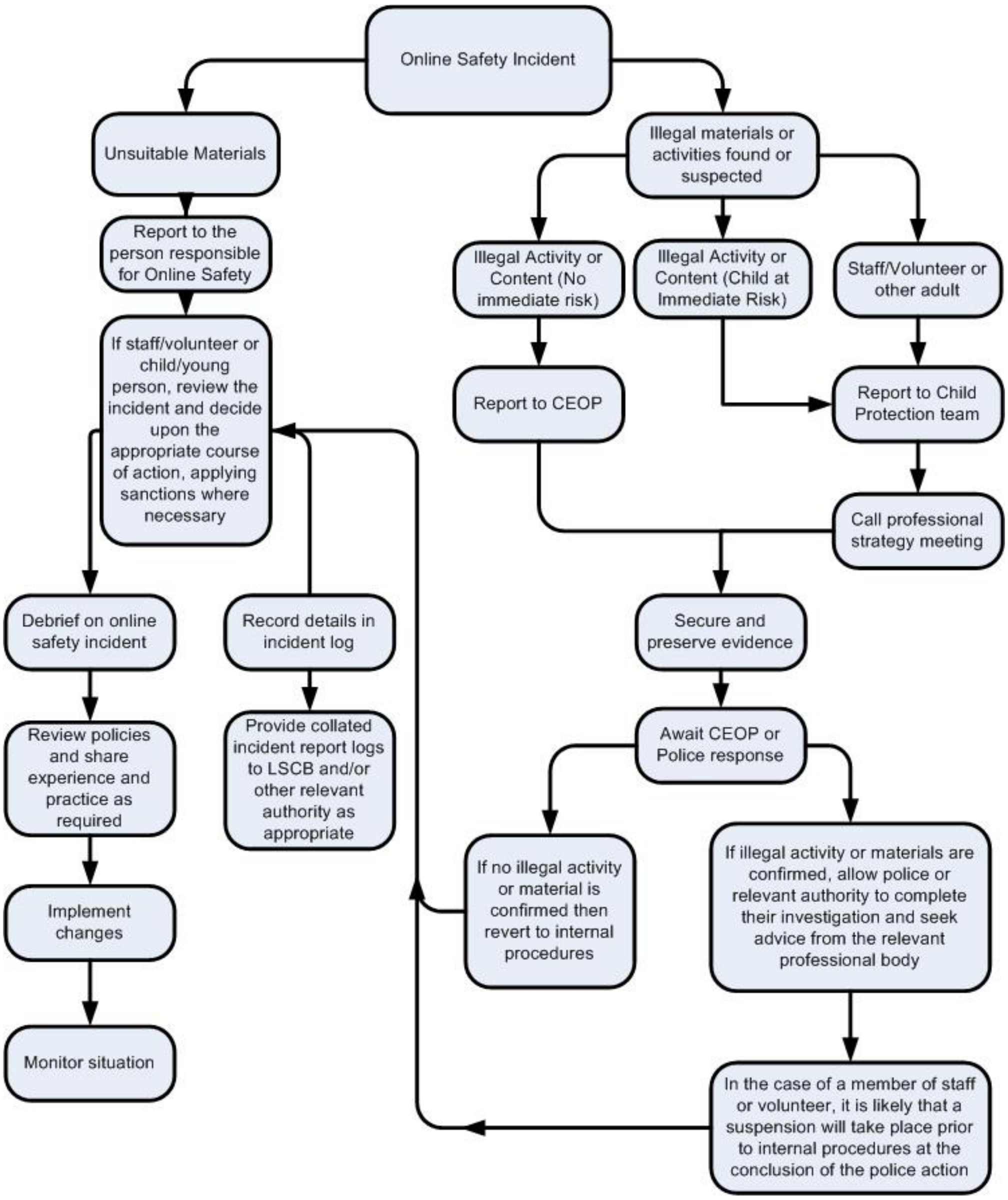
- No reference should be made in social media to students / pupils, parents / carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school or local authority
- Security settings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


Online Safety Incident
Unsuitable Materials
Report to the person responsible for Online Safety
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Debrief on online safety incident
Review policies and share experience and practice as required
Implement changes
Monitor situation
Record details in incident log
Provide collated incident report logs to LSCB and/or other relevant authority as appropriate
Illegal materials or activities found or suspected
Illegal Activity or Content (No immediate risk)
Illegal Activity or Content (Child at Immediate Risk)
Staff/Volunteer or other adult
Report to CEOP
Report to Child Protection team
Call professional strategy meeting
Secure and preserve evidence
Await CEOP or Police response
If no illegal activity or material is confirmed then revert to internal procedures
If illegal activity or materials are confirmed, allow police or relevant authority to complete their investigation and seek advice from the relevant professional body
In the case of a member of staff or volunteer, it is likely that a suspension will take place prior to internal procedures at the conclusion of the police action

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.