Engage MAT

Esafety Policy

Date of ratification: January 2018….

Date of review: January 2019……..

Esafety Policy

Introduction

The Engage Trust recognises that ICT and the internet are fantastic tools for learning and communication that can be used in schools to enhance the curriculum, challenge students, and support creativity and independence. Using ICT to interact socially and share ideas can benefit everyone in the school community, but it is important that the use of the internet and ICT is seen as a responsibility and that students, staff and parents use it appropriately and practice good e-safety. It is important that all members of the school community are aware of the dangers of using the internet and how they should conduct themselves online.

E-safety covers the internet but it also covers mobile phones and other electronic communications technologies. We know that some adults and young people will use these technologies to harm children. The harm can include sending hurtful or abusive texts and emails, attempts to radicalise via the internet and social media enticing children to engage in sexually harmful conversations or actions online, webcam filming, photography or face-to-face meetings. There is a 'duty of care' for any person working with children, and the risks and responsibilities of e-safety fall under this duty. It is important that there is a balance between controlling access to the internet and technology and allowing freedom to explore and use these tools to their full potential. This policy aims to be an aid in regulating ICT activity in schools and to provide a good understanding of appropriate ICT use that members of the school community can use as a reference for their conduct online outside of school hours. E-safety is a whole-school issue and responsibility.

Cyber-bullying by students/ staff will be treated as seriously as any other type of bullying and will be managed through our behaviour and disciplinary procedures.

1. Roles and Responsibility

The following section outlines the e-safety roles and responsibilities of individuals and groups within the Engage Trust.

The Engage Trust Network Manager is:

- Ian Wooltorton

The School's E-Safety Coordinators are:

- Lesley Moore – XLT Data Leader
- The Pinetree School Esafety Coordinator is : Mark Cresswell

Esafety Policy

The Designated members of the Governing Bodies responsible for E-Safety are:

- John Rous Milligan- Governing Body SSSfN
- Sue Cooke- Pinetree Governing Body

Director/Governors

Directors are responsible for the approval of the E-Safety Policy and Governors are responsible for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving termly information about e-safety incidents via the HT's report, monitoring reports throughout the year and a summary annual report. A member of each Governing body has taken on the role of E-Safety Governor.

The role of the E-Safety Governor will include:

- regular meetings with the E-Safety Co-coordinator
- regular monitoring of e-safety incident logs
- regular monitoring of filtering / change control logs
- reporting to relevant Governors committee, Headteacher and Senior Leaders

The role of the Network Manager will include:

- A duty of care for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to the Head teacher and E-Safety Co-coordinator.
- Ensuring the Headteacher and Senior Leaders are aware of the procedures to be followed in the event of a serious e- safety allegation being made against a member of staff.
- Ensuring that the Headteacher and the Designated Safeguarding Leads and E-Safety Co-coordinator and all other members of staff receive suitable training to enable them to carry out their e-safety roles.
- Ensuring that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- Ensuring that the school meets required safety technical requirements and any National E-Safety Guidance that may apply
- Ensuring that users may only access the networks and devices through a properly enforced password protection policy in which passwords are regularly changed
- Ensuring that the filtering policy is applied
- Ensuring that they keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant
- Ensuring that the use of the network / internet / Virtual Learning Environment / remote access / e-mail is regularly monitored in order that any misuse or attempted misuse can be

reported
- Ensuring that monitoring software / systems are implemented and updated

The role of the E-Safety Co-coordinator will include:

- taking day to day responsibility for e-safety issues and having a leading role in establishing and reviewing the school e-safety policies and documents
- ensuring that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place
- providing training and advice for staff
- liaison with Network Manager and 3rd party IT contractors
- receiving reports of e-safety incidents and creating a log of incidents to inform future e-safety developments
- meeting regularly with the E-Safety Governor to discuss current issues, review incident logs and filtering / change control logs
- Reporting when necessary to the Senior Leadership team.
- ensuring that they keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant

Teaching and Support Staff

Teaching and support staff are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and the current school e-safety policy and practices
- they have read, understood and signed the mandatory USB Stick Agreement
- that they report any suspected misuse or problem to the E–Safety Co-coordinator for investigation / action
- all digital communications with students / parents / carers will be on a professional level and only carried out using school systems
- e-safety issues are embedded in all aspects of the curriculum and other activities
- students understand and follow the e-safety and ICT Code of Conduct for Pupils
- students 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 and implement current policies with regard to these devices
- in lessons where internet use is pre-planned students are guided to sites that have been checked as suitable and that processes are in place for dealing with any unsuitable material that is found in internet searches

Designated Safeguarding Leads

Should be trained in e-safety issues and be aware of the potential serious safeguarding / child protection 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

It is important to emphasise that these are child protection issues and that the technology provides additional means for child protection issues to develop.

Students

- are responsible for using the school digital technology systems in accordance with the ICT Code of Conduct for Pupils
- have an 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 school rules on the use of mobile devices and digital cameras
- will be expected to know and understand school rules 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 school's E-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 / mobile devices in an appropriate way.

The school will take every opportunity to help parents/carers understand these issues through parents' events, leaflets, letters, website, and information about national / local e-safety campaigns and literature.

Parents and carers will be encouraged to support the school in promoting good e-safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school
- their children's personal devices in the school

2. Communicating School Policy

This policy is available from the Trust Office at Drayton, schools websites and from the school office on request for parents/carers, staff, and students to access. Rules relating to the school code of conduct when online, and e-safety guidelines, are displayed around the school. E-safety is integrated into the curriculum in any circumstance where the internet or technology are being used, and during PSHE lessons where personal safety, responsibility, and/or development are being discussed.

Parents and carers play an essential role in the education of their children and in the monitoring / regulation of the children's on-line behaviours. We will therefore seek to provide information and awareness to parents and carers through curriculum activities, the website and high profile events and campaigns e.g. Safer Internet Day.

3. Training

Staff: It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy.

- Training will be offered as follows: annually for all staff
- All new staff will receive e-safety information as part of their induction programme, directing them to read and sign the school's E-safety policy and Codes of Conduct (ICT and USB stick)
- Inset days and in meetings required
- E-Safety updates will be presented via weekly staff bulletins.
- the E-Safety Co-coordinator will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations

Governors: Governors will be invited to take part in e-safety training / awareness sessions. This may be offered in a number of ways:

- attendance at external training courses
- participation in school training / information session for staff or parents
- receipt of weekly staff bulletin

4. Making use of ICT and the Internet in School

ICT is used in school to raise educational standards, to promote student achievement, to support the professional work of staff and to enhance the school's management functions. Technology is advancing rapidly and is now a huge part of everyday life, education and business. We want to equip our students with all the necessary ICT skills that they will need in order to enable them to progress confidently into a professional working environment when they leave school.

Some of the benefits of using ICT and the internet in schools are:

For students:

- Unlimited access to worldwide educational resources and institutions such as art galleries, museums and libraries.
- Contact with schools in other countries resulting in cultural exchanges between students all over the world.
- Access to subject experts, role models, inspirational people and organisations.
- The internet can provide a great opportunity for students to interact with people that they otherwise would never be able to meet.
- An enhanced curriculum; interactive learning tools; collaboration, locally, nationally, and globally; self-evaluation; feedback and assessment; updates on current affairs as they happen.
- Access to learning whenever and wherever convenient.
- Freedom to be creative.
- Freedom to explore the world and its cultures from within a classroom.
- Social inclusion, in class and online.
- Access to case studies, videos and interactive media to enhance understanding.
- Individualised access to learning.

For staff:

- Professional development through access to national developments, educational materials and examples of effective curriculum practice and classroom strategies.
- Immediate professional and personal support through networks and associations.
- Improved access to technical support.
- Ability to provide immediate feedback to students and parents.
- Class management, attendance records, schedule, and assignment tracking.

For parents:

- The majority of communication between the schools and parents/carers is via telephone but text messages and letters will also inform parent/carers of details relating to attendance, transport and behaviour.

5. Learning to Evaluate Internet Content

With so much information available online it is important that students learn how to evaluate internet content for accuracy and intent. This is approached by the schools as part of digital literacy across all subjects in the curriculum.

Students will be taught:

- to be critically aware of materials they read, and shown how to validate information before accepting it as accurate
- to use age-appropriate tools to search for information online
- to acknowledge the source of information used and to respect copyright.

Plagiarism is against the law and the schools will take any intentional acts of plagiarism very seriously. Students who are found to have plagiarised will be disciplined. If they have plagiarised in an exam or a piece of coursework, they may be prohibited from completing that exam.

The school will also take steps to filter internet content to ensure that it is appropriate to the age and maturity of students. If staff or students discover unsuitable sites then the URL will be reported to the school E-Safety Co- coordinator or Network Manager. Any material found by members of the school community that is believed to be unlawful will be reported to the appropriate agencies.

6. Managing Information Systems

The Network Manger is responsible for reviewing and managing the security of the computers and internet networks as a whole and takes the protection of Trust data and personal protection of our school communities very seriously. This means protecting the school networks, as far as is practicably possible, against viruses, hackers and other external security threats. The security of the Trust's information systems and users will be reviewed regularly and virus protection software will be updated regularly. Some safeguards that the Trust takes to secure our computer systems are:

- Making sure that unapproved software is not downloaded to any school computers.

- Files held on the schools network will be regularly checked for viruses ; Antivirus software is installed on all school PC's
- the use of user logins and passwords to access the school network will be enforced
- Portable media (USB sticks, CDs, etc.) containing school data or programmes will not be taken off-site without specific permission from a member of the senior leadership team.

For more information on data protection in school please refer to our Data Protection policy.

7. E-mails

The Trust uses email internally for staff and students, and externally for contacting parents and other agencies, and is an essential part of Trust communication. It is also used to enhance the curriculum by:

- Providing immediate feedback on work, and requests for support where it is needed.

Staff and students must be aware that Trust/school email accounts must only be used for school-related matters, i.e. for staff to contact parents, students, other members of staff and other professionals for work purposes. This is important for confidentiality. The school has the right to monitor emails and their contents but will only do so if it feels there is reason to.

7.2 Use of BCC, CC and Reply to All

Staff using Email should ensure that they are aware of the difference between BCC and CC and that caution is used when "replying to all" to ensure that information is not shared accidentally with those not relevant.

7.3 School E-mail Accounts and Appropriate Use

Staff should only use official Trust/school-provided email accounts to communicate with students, parents or carers. Staff should not use official Trust/school provided email accounts for personal communications. Personal email accounts should not be used to contact any of these people for school business.

Emails sent from Trust/school accounts should be professionally and carefully written. Staff are representing the Trust at all times and should take this into account when entering into any email communications.

Staff must tell their manager or a member of the senior leadership team if they receive any offensive, threatening or unsuitable emails either from within the Trust/school or from an external account. They should not attempt to deal with this themselves.

The forwarding of chain messages is not permitted within the Trust.

Students will be educated through the ICT curriculum to identify spam, phishing and virus emails and attachments that could cause harm to the school network or their personal account or wellbeing.

8. Published Content and Websites

The Trust/school websites are viewed as useful tools for communicating our ethos and practice to the wider community. It is also a valuable resource for parents/carers, students, and staff for keeping up-to-date with school news and events, celebrating whole-school achievements and personal achievements, and promoting school projects.

The websites are in the public domain, and can be viewed by anybody online. Any information published on the websites will be carefully considered in terms of safety for the school community, copyrights and privacy policies. No personal information on staff or students will be published, and details for contacting the Trust/ school will be for the Trust/school office only

8.2 Policy and guidance of safe use of student's photographs and work

Photographs and students work bring our schools to life, showcase our student's talents, and add interest to publications both online and in print that represent the schools. However, the Trust/schools acknowledges the importance of having safety precautions in place to prevent the misuse of such material.

The Trust schools believe that celebrating the achievement of children in school is an important part of their learning experience and personal development. Taking photographs and videos of students for internal display and displaying student work for educational use enables us to celebrate individual and group successes as a school community.

However, we would also like to use photographs and videos of the schools and its students externally for promotional purposes (in the public domain) and to promote the good educational practice of the schools. However, in accordance with the Data Protection Act 1998 we will only do this with parent/carer consent. On admission to the school parents/carers will be asked to sign a

Home School Agreement which incorporates digital/video permissions.

By signing this form parents/carers will be consenting to the use of images of their child being used in the following outlets:

- all school publications
- on the school website
- in newspapers as allowed by the school
- in videos made by the school or in class for school projects

The form covers consent for the duration of the child's time at the school. Once the child leaves the school, photographs and videos will be archived within the school and will not be re-published without renewed consent.

Students' full names will never be published externally with their photographs, but may be published internally (for example, on display with their work).

Using photographs of individual children

The vast majority of people who take or view photographs or videos of children do so for entirely innocent, understandable and acceptable reasons. Sadly, some people abuse children through taking or using images, so we must ensure that we have some safeguards in place.

It is important that published images do not identify students or put them at risk of being identified. Only images created by or for the schools will be used in public and children may not be approached or photographed while in school or doing school activities without the school's permission.

The schools follow general rules on the use of photographs of individual children:

- Parental consent must be obtained for external/promotional use.
- Electronic and paper images will be stored securely.
- Images will be carefully chosen to ensure that they do not pose a risk of misuse. This includes ensuring that students are appropriately dressed. Photographs of activities which may pose a greater risk of potential misuse (for example, swimming activities) will focus more on the sport than the students (i.e. a student in a swimming pool, rather than standing by the side in a swimsuit).
- For public documents, including in newspapers, full names will not be published alongside images of the child. Groups may be referred to collectively by year group or class name.
- Events recorded by family members of the students such as school plays or sports days must be used for personal use only and not be posted on any social media sites

Students are encouraged to tell a member staff if they are concerned or uncomfortable with any photographs that are taken of them or in which they are being asked to participate.

Any photographers that are commissioned by the schools will be fully briefed on appropriateness in terms of content and behaviour, will wear identification at all times, and will not have unsupervised access to the students and will abide by guidelines as per our Visitor Policy.

For more information on safeguarding in schools please refer to our school Safeguarding and Child protection policy.

8.3 Complaints of misuse of photographs or video

Parents/ carers should follow the standard school complaints procedure, accessible via the website, if they have a concern or complaint regarding the misuse of school photographs.

8.4 Social networking, social media and personal publishing

Personal publishing tools include blogs, wikis, social networking sites, Skype, bulletin boards, chat rooms and instant messaging programmes.

These online forums are the more obvious sources of inappropriate and harmful behaviour and where students are most vulnerable to being contacted by a dangerous person. It is important that we educate students so that they can make their own informed decisions and take responsibility for their conduct online.

Social media sites have many benefits for both personal use and professional learning; however, both staff and students should be aware of how they present themselves online. Students are taught through the ICT curriculum and PSHE about the risks and responsibility of uploading personal information and the difficulty of taking it down completely once it is out in such a public place.

Students are educated on the dangers of social networking sites and how to use them in safe and productive ways. They are all made fully aware of the school's code of conduct regarding the use of ICT and technologies and behaviour online.

Any sites that are to be used in class will be risk-assessed by the teacher in charge prior to the lesson to ensure that the site is age-appropriate and safe for use.

Official school blogs created by staff or students/year groups/school clubs as part of the school curriculum will be password-protected and run with the approval of a member of staff and will be moderated by a member of staff.

Students and staff are encouraged not to publish specific and detailed private thoughts, especially those that might be considered hurtful, harmful or defamatory. The Trust expects all staff and students to remember that they are representing the school at all times and must act appropriately.

Safe and professional behaviour of staff online will be discussed at staff safeguarding training.

9. Mobile Phones and Personal Devices

While mobile phones and personal communication devices are common place in today's society, their use and the responsibility for using them should not be taken lightly. Some issues surrounding the possession of these devices are:

- they can make students and staff more vulnerable to cyberbullying
- they can be used to access inappropriate internet material
- they can be a distraction in the classroom
- they are valuable items that could be stolen, damaged, or lost
- They can have integrated cameras, which can lead to child protection, bullying and data protection issues.

The schools therefore do not allow mobile devices to be used by students during the school day; if this occurs, the devices will be stored securely and returned at end of day.

In circumstances where there is a suspicion that material on a device/phone is possibly illegal or in connection with illegal acts, the device/ phone will be handed to the Police for further investigation.

We do however, understand that a parent/carer may wish for their child to have a mobile phone for their journey to and from school.

Emergencies

If a student needs to contact his parents/carers they will be allowed to use a school phone.

If parents/carers need to contact their child urgently they should phone the school office and a message will be relayed promptly.

The Trust accepts no responsibility whatsoever for theft, loss or damage relating to phones/devices

including those handed in/confiscated. The Trust/school will not investigate theft, loss or damage relating to phones/devices.

Under no circumstances should staff use their own personal devices to contact students or parents either in or out of school time unless in an emergency. Staff are not permitted to take photos or videos of students on their own devices. If photos or videos are being taken as part of the school curriculum or in a professional capacity, the school equipment must be used.

The Trust expects staff to lead by example. Personal mobile phones should be switched off or on 'silent' during school hours.

With the authorisation of the local Head teacher, some teams may use their personal mobile phones to make calls, texts or WhatsApp group in order to ensure effective communication or to ensure pupil or staff safety.

Any breach of policy may result in disciplinary action against that member of staff.

10. Cyberbullying

Cyberbullying, as with any other form of bullying, is taken very seriously by the Trust/school. Information about specific strategies or programmes in place to prevent and tackle bullying are set out in the Anti-bullying policy. The anonymity that can come with using the internet can sometimes make people feel safe to say and do hurtful things that they otherwise would not do in person. It is made very clear to members of the Trust community what is expected of them in terms of respecting their peers, members of the public and staff, and any intentional breach of this will result in disciplinary action.

If an allegation of bullying does come up, the Trust/ school will:

- take it seriously
- act as quickly as possible to establish the facts.
- it may be necessary to examine school systems and logs or contact the service provider in order to identify the bully
- record and report the incident
- provide support and reassurance to the victim
- make it clear to the 'bully' that this behaviour will not be tolerated.

If there is a group of people involved, they will be spoken to individually and as a whole group. It is important that children who have harmed another, either physically or emotionally, redress their actions and the schools will make sure that they understand what they have done and the impact of

their actions.

If a sanction is used, it will correlate to the seriousness of the incident and the 'bully' will be told why it is being used. They will be asked to remove any harmful or inappropriate content that has been published, and the service provider may be contacted to do this if they refuse or are unable to remove it. They may have their internet access suspended.

Repeated bullying may result in a fixed-term exclusion or disciplinary action.

11. Managing Emerging Technologies

Technology is progressing rapidly and new technologies are emerging all the time. The Network Manager, in liaison with Esafety coordinator, will risk-assess any new technologies before they are allowed in school, and will consider any educational benefits that they might have. The school keeps up-to-date with new technologies and is prepared to quickly develop appropriate strategies for dealing with new technological developments.

12. Protecting Personal Data

The Engage Trust believes that protecting the privacy of our staff, Governors and students and regulating their safety through data management, control and evaluation is vital. The Trust/schools collect personal data from students, parents, governors and staff and process it in order to support teaching and learning, monitor and report on student and teacher progress, provide information to Government and to strengthen our pastoral provision.

We take responsibility for ensuring that any data that we collect and process is used correctly and only as necessary. Assessment results, attendance and registration records, special educational needs data, and any relevant medical information are examples of the type of data that the school needs. Through effective data management we can monitor a range of provisions and evaluate the wellbeing and academic progression of our school community to ensure that we are doing all we can to support both staff and students.

In line with the Data Protection Act 1998, and following principles of good practice when processing data, the Trust/school will:

- ensure that data is fairly and lawfully processed
- process data only for limited purposes
- ensure that all data processed is adequate, relevant and not excessive
- ensure that data processed is accurate
- not keep data longer than is necessary

- process the data in accordance with the data subject's rights
- ensure that data is secure
- ensure that data is not transferred to other countries outside the EU without adequate protection.

There may be circumstances where the Trust/school is required either by law or in the best interests of our students or staff to pass information onto external authorities; for example, our local authority, Ofsted, or the Department of Health.

These authorities are up-to-date with data protection law and have their own policies relating to the protection of any data that they receive or collect. For more information on the Trust's safeguards relating to data protection please read the Data protection policy.

12.2 Password Security

Many Trust/school systems for staff and students require the use of a password. All staff and students are supported to adhere to the following password guidelines:

- Never write passwords down.
- Never send a password through email.
- Never tell anyone your password.
- Never reveal your password over the telephone.
- Never hint at the format of your password.
- Don't auto save passwords e.g. in a browser.
- Never reveal or hint at your password on a form on the internet.
- Report any suspicion of your password being broken to the Network Manager.
- Don't use common acronyms as part of your password.
- Don't use common words or reverse spelling of words in part of your password.
- Don't use names of people or places as part of your password.
- Don't use part of your login name in your password.
- Don't use parts of numbers easily remembered such as phone numbers, social security numbers, or street addresses.
- Be careful about letting someone see you type your password.

Staff should ensure that they lock their computer, even if leaving it for a short time, and that they log off at the end of a session.

13. Unsuitable / inappropriate activities

Some internet activity e.g. accessing child abuse images or disturbing racist material is illegal and would obviously be banned from Trust/ school and all other technical systems. Other activities e.g. cyber-bullying are banned and could lead to criminal prosecution. There are, however, a range of activities which may, generally, be legal but would be inappropriate in a Trust/school context, either because of the age of the user or the nature of those activities. The following activities would be inappropriate in our context:

- pornography
- promotion of any kind of discrimination and radicalisation
- threatening behaviour, including promotion of physical violence, torture ,mental harm and FGM
- any other information which may be offensive to colleagues or breaches the integrity of the ethos of the schools or brings the schools into disrepute
- using Trust/school systems to run a private business
- using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the Trust
- infringing copyright
- revealing or publicising confidential or proprietary information e.g. financial, personal information, data bases, computer / network access codes and passwords
- creating or propagating computer viruses or other harmful files
- unfair usage, downloading or storing information for personal use
- non-educational on-line gaming,
- on-line gambling
- use of social media without permission

- use of messaging apps without permission
- use of videoing broadcasting or YouTube without permission

13.1 Responding to incidents of misuse

It is hoped that all members of the Trust/school community will be responsible users of digital technologies, who understand and follow 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:

The Network Manager in liaison with senior members of staff should be involved in the process and it will remain confidential. This is vital to protect individuals if accusations are subsequently reported.

The Network login will be disabled by Network Manager and the device will be quarantined where appropriate

The procedure should be conducted using a designated computer that will not be used by anyone else and if necessary can be taken off site by the police should the need arise. The same computer should be used for the duration of the process.

Relevant staff will be able to access the Internet to conduct the procedure, and can draw down history from the Network or device if requested.

The URL of any site containing the alleged misuse and the nature of the content causing concern will be recorded.

In such cases it is important that all of the above steps are taken as they will provide an evidence trail.

Once fully investigated the group should 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 Local Authority or national / local organisations (as relevant)
- Police involvement and / or action

If the review indicates child abuse then the monitoring should be halted and referred to MASH and the Police immediately. Other instances to report to the police would include:

- Incidents of 'grooming' behaviour including attempts to radicalise
- 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 material

School actions and sanctions

It is more likely that the Trust/ 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 an appropriate 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