Twickenham Preparatory School
Nurturing, Inspiring, Successful

Online Safety Policy
Whole School Policy including EYFS

"Twickenham Preparatory School seeks to create a safe, caring and happy Christian environment in which all pupils are valued and can thrive personally, socially and academically."

Date Revised:	January 2020
Approval Body:	Board of Governors
Authorised by Chair of Governors:	
Date Approved:	6th February 2020
Review Schedule:	Annually
Circulation:	Governors, all staff, parents, pupils, volunteers

Contents

1. Scope

This policy applies to all members of the school community (including staff, pupils, volunteers, parents/carers) who have access to and are users of school digital technology systems, both in and out of the School.

2. Objectives

- To ensure that pupils are appropriately supervised during school activities
- To promote responsible behaviour with regard to online based activities
- To take account and adhere to legislative guidance, in particular the General Data Protection Regulations and the Data Protection Act 2018.

3. Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within the School.

3.1. Board of Governors

The Board of Governors is responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Board of Governors and the Education Committee receiving regular information about online safety incidents and monitoring reports.

3.2. Head and Senior Leadership Team (SLT)

- The Head and the SLT 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
- The Head and the Deputy Head 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
- The Head is responsible for ensuring that the Online Safety Co-ordinator and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant
- The Head 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
- The Senior Leadership Team will receive regular monitoring reports from the Online Safety Co-ordinator.

3.3. Online Safety Co-ordinator

The role of the Online Safety Co-ordinator is undertaken by the Head of ICT & Computing. The Online Safety Co-ordinator:

- Takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online policies/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 school technical staff
- Receives reports of online safety incidents and creates a log of incidents to inform future online safety developments

- Meets regularly with the Designated Safeguarding Lead (DSL) to discuss current issues, review incident logs and filtering/change control logs
- Attends relevant committee meetings as required
- Reports regularly to the Head and SLT.

3.4. Network Consultant

The Network Consultant (Brandtek Ltd) is responsible for ensuring:

- That the school's technical infrastructure is secure and is not open to misuse or malicious attack
- That the School meets required online safety technical requirements and any local authority/other relevant body online safety policy/guidance that may apply
- That users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- 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
- That the use of the network (including internet, learning platform, remote access and email) is regularly monitored in order that any misuse/attempted misuse can be reported to the Head and the Online Safety Co-ordinator for investigation
- That software updates/patches are installed on a timely basis as they become available
- That monitoring software/systems are implemented and updated as agreed.

3.5. Teaching and Support Staff

Are responsible for ensuring that:

- They have an up to date awareness and understanding of E-Safety matters and of the current school Online Safety Policy
- They have read, understood and signed the staff I.T. Acceptable Use Policy
- They report any suspected misuse or problem to the Head, SLT or Online Safety Co-ordinator for investigation
- All digital communications with pupils, parents and 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 Pupil Acceptable Use Agreement
- 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.

3.6. Designated Safeguarding Lead (DSL) and Deputy DSL

The DSL and Deputy DSL should 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 online contact with adults/strangers
- Potential or actual incidents of grooming or radicalisation
- Online bullying.

3.7. Pupils

- Are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Policy
- 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 guidelines on the use of mobile devices and digital cameras. They should also know and understand policies on the taking /use of images and on online-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.

3.8. Parents and Carers

Parents and carers play a crucial role in ensuring that their children understand the need to use the internet and mobile devices in an appropriate way. The School will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website/Learning Platform 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 school website
- Their children's personal devices in the School (where this is permitted).

4. Policy Statements

4.1. 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 and digital literacy is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the 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 will be provided as part of Computing/PHSE/other lessons 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 supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making
- Pupils should be helped to understand the need for the Pupil Acceptable Use Agreement 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 they visit
- It is accepted that from time to time, for good educational reasons, pupils may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Online Safety Co-ordinator arranges to 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.

4.2 Education: Parents and 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/regulation of the children's online 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.

The School will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters, newsletters and the school's website
- Parents/Carers evenings/sessions
- High profile events/campaigns e.g. Safer Internet Day
- Reference to the relevant web sites/publications
  e.g. swgfl.org.uk www.saferinternet.org.uk/ http://www.childnet.com/parents-and-carers

4.3 Education: The Wider Community

The School will provide opportunities for members of the school's community to gain from the school's online safety knowledge and experience. This may be offered through the following:

- Providing family learning events in use of new digital technologies, digital literacy and online safety

- Online safety messages targeted towards grandparents and other relatives as well as parents

4.4 Education and Training: Staff and Volunteers

It is essential that all 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 will receive online safety training as part of their induction programme, ensuring that they fully understand the school's Online Safety Policy and Acceptable Use Agreements
- It is expected that some staff will identify online safety as a training need within the performance management process
- The Online Safety Co-ordinator (or other nominated person) 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/team meetings/INSET days
- The Online Safety Co-ordinator (or other nominated person) will provide advice/guidance/ training to individuals as required.

4.5 Training: Governors

Governors should take part in online safety training, with particular importance for those who are members of any subcommittee/group involved in technology/online, safety/health and safety/safeguarding.

5. Technical: Infrastructure/Equipment, Filtering and Monitoring

The Network Consultant 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.

The school's web filtering solution enables the School to filter down and monitor all online activity per individual user, whilst filtering over 100 categories.

6. Mobile Technologies

The School provides tablets to staff if a requirement of their role. Staff should understand that the primary purpose of the tablet is educational and that their use should be consistent with the I.T. Acceptable Use Policy. No personal apps or personal information should be installed on school mobile technologies and the device is for the **sole** use of the staff member. Staff are responsible for the safety and care of the tablet provided. The School reserves the right to charge staff members for repairs/replacements if damages are due to negligence.

Tablets may be provided to pupils during lessons for educational purposes. Pupils are not permitted to use personal mobile technologies during school hours, without prior authorisation from the Head.

Pupils in Reception – Year 5 are not permitted to bring mobile phones to School. Pupils in Year 6 -8 may bring a mobile phone to School if required for travel arrangements. All phones must be stored in the school office during school hours.

7. Use of Digital and Video Images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet.

However, staff, governors, volunteers, 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 e.g. on social networking sites
- Written permission from parents or carers (for pupils below Year 8) is obtained regarding the use of images. Pupils in Year 8 are able to provide their own written permission.
- 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 should not be used for such purposes
- Care should be taken when taking digital/video images that 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 school website, or elsewhere that include 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.

Further detail can be found in the school's Guidelines for Taking and Using Images of Pupils that is located on the school's website.

8. Data Protection

Personal data will be recorded, processed, transferred and made available according to the current data protection legislation.

For further information the following documents are available on the Reference Drive (R):

- Data Protection Policy
- Privacy Notices (Staff, Pupil and Parent)
- Data Retention & Storage Policy.

9. Communications

When using communication technologies, the School considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff should therefore use only the school email service to communicate with others when in School, or on school systems (e.g. by remote access)
- Users must immediately report to a senior member of staff, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication
- Any digital communication between staff and pupils or parents / carers (email, social media, chat, blogs, virtual learning environment (VLE) etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications
- Pupils should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

10. Social Media – Protecting Professional Identity

All schools have a duty of care to provide a safe learning environment for pupils and staff. Staff members who harass, engage in online bullying, discriminate on the grounds of sex, race or disability, or who defame a third party may render the School liable to the injured party.

The School provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the School through:

- Ensuring that personal information is not published
- Training is provided including: 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.

School staff should ensure that:

- No reference should be made (on personal social media accounts) to pupils, parents/carers, school staff, governors, volunteers, contractors or consultants
- 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
- Security settings on personal social media profiles should be regularly checked to minimise risk of loss of personal information.

When official school social media accounts are established there is:
- A process for approval by the Business Manager (responsible for the data protection in the School), SLT and the Board of Governors
- Clear processes for the administration and monitoring of these accounts

Personal Use
- Personal communications are those made via a personal social media account. In all cases, where a personal account is used which associates itself with the School or impacts on the School, it must be made clear that the member of staff is not communicating on behalf of the School with an appropriate disclaimer. Such personal communications are within the scope of this policy
- Personal communications which do not refer to or impact upon the School are outside the scope of this policy
- Where excessive personal use of social media in School is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
- The School permits reasonable and appropriate access to private social media sites.

Monitoring of Public Social Media
- As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the School
- The School should effectively respond to social media comments made by others according to a defined process.

11. Dealing with Unsuitable/Inappropriate Activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from School and all other technical systems. Other activities e.g. cyber bullying are also 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 school context, either because of the age of the users or the nature of those activities.

The School believes that the activities referred to below would be inappropriate in a school context and that users, should not engage in these activities in or outside the School when using school equipment or systems.

The school policy restricts usage as follows:

Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:
- Child sexual abuse images
- Grooming, incitement, arrangement or facilitation of sexual acts against children
- Possession of an extreme pornographic image
- Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation)
- Pornography

- Promotion of any kind of discrimination
- Threatening behaviour, including promotion of physical violence or mental harm
- Promotion of extremism or terrorism
- Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the School or brings the School into disrepute.

Additional restrictions include:

- Using school systems to run a private business
- Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the School
- Infringing copyright
- Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)
- Creating or propagating computer viruses or other harmful files
- Unfair usage (downloading / uploading large files that hinders others in their use of the internet)
- Online gaming (educational/non-educational)
- Online gambling
- Online shopping for personal use and during school hours
- File sharing
- Use of social media for personal use
- Use of messaging apps
- Use of video broadcasting for personal use e.g. Youtube.

12. Responding to Incidents of Misuse

12.1. 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 **(Appendix 1)** for responding to online safety incidents and report immediately to the police.

12.2 Other Incidents

It is hoped that all members of the school 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 member of the SLT 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 pupils 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 Local Authority
  - 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
- promotion of terrorism or extremism
- other criminal conduct, activity or materials

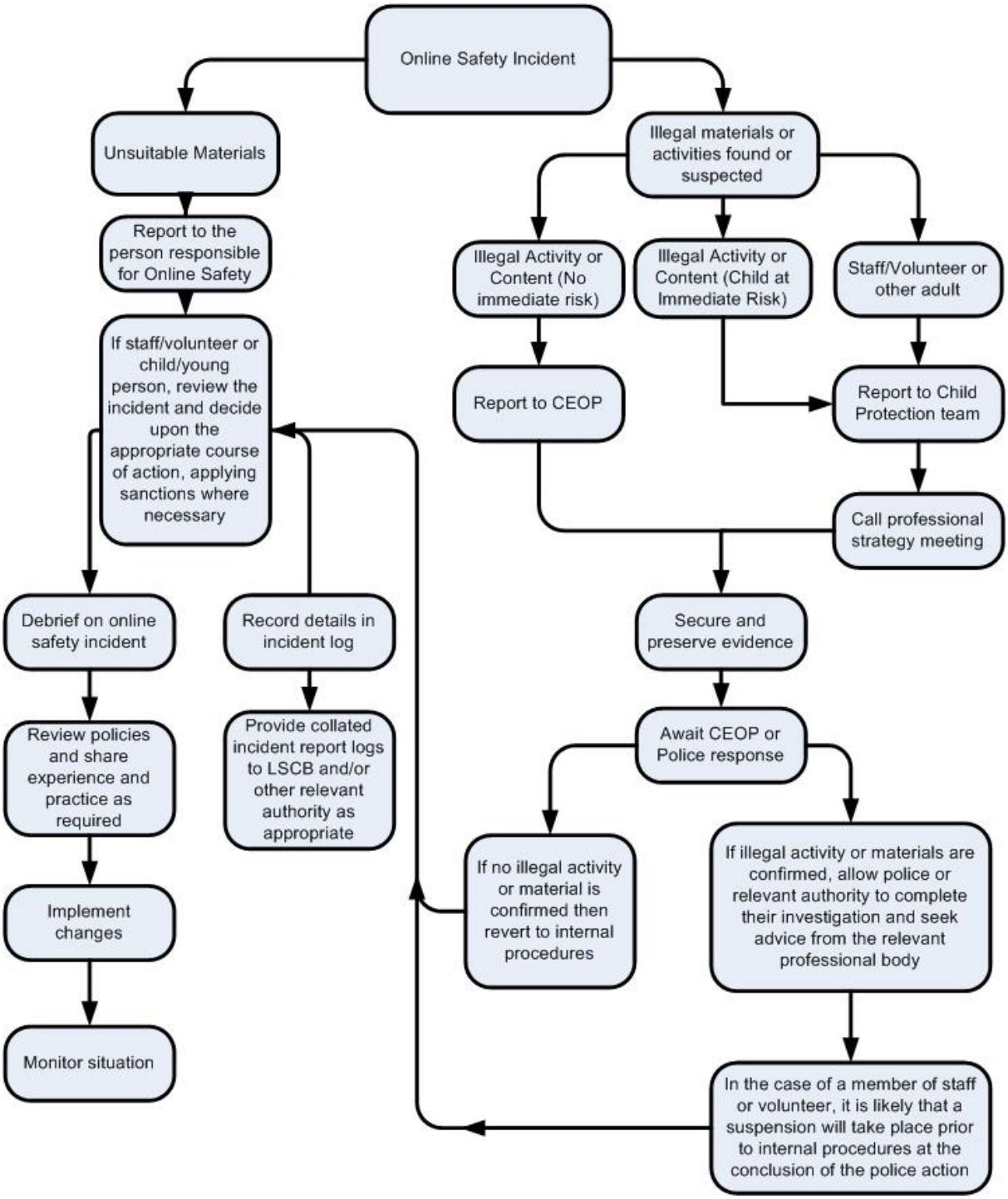
If an incident is reported to the police the computer in question should be isolated as best as is possible. Any change to its state may hinder a later police investigation.

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 safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

12.3 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: Responding to Online Safety Incidents



CEOP: Child Exploitation and Online Protection Centre
CEOP is a law enforcement agency whose aim is to help keep children and young people safe from sexual abuse and grooming online.