Torquay Girls' Grammar School E-Safety Policy

Background / Rationale

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school.

The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and *students / pupils* learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe internet access at all times.

The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. A school e-safety policy should help to ensure safe and appropriate use. The development and implementation of such a strategy should involve all the stakeholders in a child's education from the headteacher and governors to the senior leaders and classroom teachers, support staff, parents, members of the community and the students / pupils themselves.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil / student achievement.

However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

Many of these risks reflect situations in the off-line world and it is essential that this e-safety policy is used in conjunction with other school policies (eg behaviour, anti-bullying and child protection policies).

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build students' / pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.
The school must demonstrate that it has provided the necessary safeguards to help ensure that they have done everything that could reasonably be expected of them to manage and reduce these risks. The e-safety policy that follows explains how we intend to do this, while also addressing wider educational issues in order to help young people (and their parents / carers) to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

Development / Monitoring / Review of this Policy

This e-safety policy has been developed by the E Safety Committee) made up of:

- School E-Safety Coordinator / Officer
- Senior Leader Child Protection
- School teaching & support Staff
- ICT Technical staff
- Governors
- Students

Consultation with the whole school community has taken place through the following:

- Staff meetings
- Student Council
- Governors meeting / sub committee meeting
- Parents evening
- School website / newsletters

Schedule for Development / Monitoring / Review

This e-safety policy was approved by the *Governing Body / Governors Sub Committee on:*	
The implementation of this e-safety policy will be monitored by the:	*E-Safety Committee*
Monitoring will take place at regular intervals:	*Annually*
The *Governing Body / Governors Sub Committee* will receive a report on the implementation of the e-safety policy generated by the monitoring group (which will include anonymous details of e-safety incidents) at regular intervals:	*Annually*
The E-Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place. The next anticipated review date will be:	*May 2018*
Should serious e-safety incidents take place, the following external persons / agencies should be informed:	*Chair of the Governing Body*

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited)
- Internal monitoring data for network activities
- Surveys / questionnaires of students

Scope of the Policy

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

The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students / 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 e-safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

The school 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 e-safety behaviour that take place out of school.

Roles and Responsibilities

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

Governors:

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the *Governors / Governors Sub Committee* receiving information about e-safety incidents and monitoring reports. A member of the Governing Body has taken on the role of *E-Safety Governor* The role of the E-Safety Governor (Mrs Michelle Wilson – Safeguarding Governor) will include:

- regular meetings with the E-Safety Co-ordinator / Officer
- reporting to relevant Governors committee / meeting

Headteacher and Senior Leaders:

- The Headteacher is responsible 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 E-Safety Co-ordinator / Officer;
- The Headteacher / Senior Leaders are responsible for ensuring that the E-Safety Coordinator / Officer and other relevant staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, as relevant;
- The Headteacher and another member of the Senior Leadership Team / Senior Management Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff;
- The Headteacher / Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles;
- The Senior Leadership Team will receive monitoring reports from the E-Safety Co-ordinator.

E-Safety Coordinator / Officer:

(It is strongly recommended that each school should have a named member of staff with a day to day responsibility for e-safety, some schools may choose to combine this with the Child Protection Officer role. Schools may choose to appoint a person with a child welfare background, preferably with good knowledge and understanding of the new technologies, rather than a technical member of staff – but this will be the choice of the school)

Designated E-Safety Co-ordinators - (Gordon Neighbour / Andrew Walker)

- leads the e-safety committee
- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- provides training and advice for staff
- liaises with school ICT technical staff
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments.
- meets regularly with E-Safety Governor to discuss current issues.
- attends relevant meeting / committee of Governors
- reports to Senior Leadership Team

Network Manager / Technical staff:

The Network Manager / Systems Manager / ICT Technician / ICT Co-ordinator is responsible for ensuring:

- that the school's ICT infrastructure is secure and is not open to misuse or malicious attack.
- that the school meets the e-safety technical requirements outlined in the Best Practice Documents produced by the SWGfL.
- that users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed
- M247 is informed of issues relating to the filtering applied by the school.
- the school's filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person.
- that he / she keeps 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.
- that the use of the network / Virtual Learning Environment (VLE) / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the E-Safety Co-ordinator for investigation.
- that monitoring software / systems are implemented and updated as required.

Teaching and Support Staff

are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices
- they have read, understood and signed the school Staff Acceptable Use Policy / Agreement (AUP)
- they report any suspected misuse or problem to the E-Safety Co-ordinator for investigation.
- digital communications with students / pupils (email / Virtual Learning Environment (VLE) / voice) should be on a professional level and only carried out using official school systems
- they are aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices
- in lessons where Internet use is pre-planned students 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;
- Staff should act as good role models in their use of digital technologies, the Internet and mobile devices
- Where students are allowed to freely search the Internet, staff should be vigilant in monitoring the content of the websites that the young people visit.

Designated person for child protection / Child Protection Officer (Sarah Colombini)

should be trained in e-safety issues and be aware of the potential for serious 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

E-Safety Committee

Members of the E-safety committee (or other relevant group) will assist the E-Safety Coordinator / Officer (or other relevant person, as above) with:

- the review & monitoring of the school e-safety policy / documents.
- the production / review / monitoring of the school filtering policy and acceptable use policies.
- mapping and reviewing the e-safety curricular provision – ensuring relevance, breadth and progression.
- consulting stakeholders – including parents / carers and the students about the e-safety provision.

Students:

- are responsible for using the school ICT systems in accordance with the Student / Pupil Acceptable Use Policy, which they will be expected to sign before being given access to school systems;
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations;
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so;
- will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying;
- should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the 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 therefore take every opportunity to help parents understand these issues through a range of mediums. These could include; parents' evenings, newsletters, letters, website / VLE and information about national / local e-safety campaigns. Parents and carers will be responsible for:

- endorsing (by signature) the Student / Pupil Acceptable Use Policy;
- digital and video images taken at school events;
- Their children's personal devices in the school.

Community Users

Community Users who access school ICT systems / website / VLE as part of the Extended School provision will be expected to sign the staff acceptable Community AUP before being provided with access to school systems.

Policy Statements

Education – students / pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students in e-safety is therefore an essential part of the school's e-safety provision.

E-Safety education will be provided in the following ways:

- A planned e-safety programme should be provided as part of ICT & PHSE / this will cover both the use of ICT and new technologies in school and outside school;
- Key e-safety messages should be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities;
- Students / pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information;
- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the Internet;
- Rules for use of ICT systems / internet will be posted in all rooms;
- Students should be helped to understand the need for the Student Acceptable Use Agreement It is accepted from time to time, for good educational reasons, students may research topics (e.g. racism, drugs, discrimination) that would normally result in Internet searches being blocked or that they may require access to site that in the normal course of events are blocked. In such a situation, staff can request the technical team *to temporarily* remove those sites from the filtered list for *the period of study*. Any request to do so should be *auditable (e.g.an email giving authorisation from the responsible member of staff)*, with *clear reasons* for the need.

Education – parents / carers

Many parents and carers have only a limited understanding of e-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 on-line experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. "There is a generational digital divide". (Byron Report).
The school will therefore seek to provide information and awareness to parents and carers through:

- *Letters, newsletters, web site, VLE*
- *Parents evenings*
- *Reference to appropriate external resources.*

Education & 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:

- A planned programme of formal e-safety training will be made available to staff. An audit of the e-safety training needs of all staff should be carried out regularly. It is expected that some staff may identify e-safety as a training need within the performance management process;
- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Policies
- The E-Safety Coordinator (or other nominated person) will receive regular updates through attendance at appropriate events and by reviewing guidance documents released by BECTA / SWGfL / LA and others.
- The E-Safety Coordinator will provide advice / guidance / training as required to individuals as required

Training – Governors

Governors should take part in e-safety training / awareness sessions, with particular importance for those who are members of any sub committee / group involved in ICT / e-safety / health and safety / child protection. This may be offered by participation in school training / information sessions for staff or parents

Technical – infrastructure / equipment, filtering and monitoring

The school 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. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities:

- School ICT systems will be managed in ways that ensure that the school meets the e-safety technical requirements outlined in the appropriate policies;
- There will be regular reviews and audits of the safety and security of school ICT systems;
- Servers, wireless systems and cabling must be securely located and physical access restricted;
- All users will have clearly defined access rights to school ICT systems;
- All users will be provided with a username and password by the network manager. Users will be required to change their password at frequent intervals.
- The "master / administrator" passwords for the school ICT system, used by the Network Manager must also be available to the Headteacher or Head of ICT and kept in a secure place (eg school safe)
- Kevin Pike (Network Manager) 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 sex abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated;
- Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security;
- The school maintains and supports the managed filtering service provided by Smoothwall;
- In the event of the Network Manager (or other person) needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Headteacher (or other nominated senior leader).
- Requests from staff for sites to be removed from the filtered list will be considered by the Network Manager and School ICT coordinator) If the request is agreed, this action will be recorded;
- School ICT technical staff regularly monitor and record the activity of users on the school ICT systems and users are made aware of this in the Acceptable Use Policy;
- Personal data can not be sent over the internet or taken off the school site unless safely encrypted or otherwise secured. (see School Personal Data Policy Template in the appendix for further detail)
- The school will endeavour to provide enhanced / differentiated user-level filtering (allowing different filtering for different ages and different groups of users);
- An appropriate system is in place for users to report any actual / potential technical incident / security breach to the e-safety co-ordinator;
- 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 anti-virus software;
- An agreed policy is in place for the provision of temporary access for guest users onto the school system.
- Staff should not attempt to download executable files unless agreed with the network manager;

- An agreed policy is in place regarding the extent of personal use that users and their family members are allowed on school devices that can be used outside of school.

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 e-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 Acceptable Use Agreement;
- All network systems are secure;
- Where possible these devices will be covered by the school's / academy's normal filtering systems, while being used on the premises;
- All users will use their username and password and keep this safe;
- Students / Pupils receive guidance on the use of personal devices;
- Monitoring of usage will take place to ensure compliance;
- Any device loss, theft, change of ownership of the device will be reporte

Use of digital and video images - Photographic, Video

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 and students need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying 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 students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet eg on social networking sites;
- Staff are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. 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 students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute;
- Students must not take, use, share, publish or distribute images of others without their permission;
- Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images;
- Students' 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 are published on the school website;
- Student's work can only be published with the permission of the student 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.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse;
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data;
- Personal data should be stored on a suitable system e.g. OneDrive or that they use end-to-end encryption if transporting data via USB stick or mobile device;

The school / academy must ensure that:

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for;
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay;
- All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing". (see Privacy Notice section in the appendix);
- It has a Data Protection Policy (see appendix for template policy);
- It is registered as a Data Controller for the purposes of the Data Protection Act (DPA);
- Responsible persons are appointed / identified - Senior Information Risk Officer (SIRO) and Information Asset Owners (IAOs);
- Risk assessments are carried out;
- It has clear and understood arrangements for the security, storage and transfer of personal data;
- Data subjects have rights of access and there are clear procedures for this to be obtained;
- There are clear and understood policies and routines for the deletion and disposal of data;
- There is a policy for reporting, logging, managing and recovering from information risk incidents;
- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties;
- There are clear guideleines about the use of cloud storage / cloud computing which ensure that such data storage meets the requirements laid down by the Information Commissioner's Office.

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks / disadvantages:

	Staff & other adults				Students / Pupils			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school	Y						Y	
Use of mobile phones in lessons		Y				Y	Y	
Use of mobile phones in social time	Y						Y	
Taking photos on mobile phones or other camera devices		Y				Y	Y	
Use of hand held devices eg PDAs, PSPs	Y					Y	Y	
Use of personal email addresses in school, or on school network	Y							Y
Use of school email for personal emails	Y				Y			
Use of chat rooms / facilities	Y					Y	Y	
Use of instant messaging	Y					Y	Y	
Use of social networking sites	Y					Y	Y	
Use of blogs	Y					Y	Y	

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 need to be aware that email communications may be monitored;
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email;
- Any digital communication between staff and students or parents / carers (email, chat, 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 public chat / social networking programmes must not be used for these communications;
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Social Media - Protecting Professional Identity

Reasonable steps to prevent predictable harm must be in place.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 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.

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 /academy or local authority;
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

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 ICT systems. Other activities e.g. Cyber-bullying would be 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 in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts certain internet usage as follows:

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
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**					P
	promotion or conduct of illegal acts, eg under the child protection, obscenity, computer misuse and fraud legislation					P
	adult material that potentially breaches the Obscene Publications Act in the UK					P
	criminally racist material in UK					P
	pornography				P	
	promotion of any kind of discrimination				P	P
	promotion of racial or religious hatred				P	P
	threatening behaviour, including promotion of physical violence or mental harm				P	
	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				P	
Using school systems to run a private business					P	
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by SWGfL and / or the school					P	
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions					P	P
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)					P	
Creating or propagating computer viruses or other harmful files					P	P
Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet					P	
On-line gaming (educational)			P			
On-line gaming (non educational)					P	
On-line gambling					P	
On-line shopping / commerce			P			
File sharing			P			

Use of social networking sites		P			
Use of video broadcasting eg Youtube		P			

Responding to incidents of misuse

It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse:

If any apparent or actual misuse appears to involve illegal activity ie.

- child sexual abuse images;
- adult material which potentially breaches the Obscene Publications Act;
- criminally racist material;
- other criminal conduct, activity or materials;

Best practice guidance should be consulted and actions followed in line with that guidance, in particular sections on reporting the incident to the police and the preservation of evidence.

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

Students	Possible actions that will be guided by the School Discipline Policy.								
Incidents:	Refer to class teacher / tutor	Refer to Head of Department / Head of Year / other	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering / security etc	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction eg detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		P	P	P					
Unauthorised use of non-educational sites during lessons		P							
Unauthorised use of mobile phone / digital camera / other handheld device	P	P							
Unauthorised use of social networking / instant messaging / personal email	P	P							
Unauthorised downloading or uploading of files					P				
Allowing others to access school network by sharing username and passwords					P		P	P	
Attempting to access or accessing the school network, using another student's / pupil's account					P	P	P	P	
Attempting to access or accessing the school network, using the account of a member of staff			P		P	P	P	P	P
Corrupting or destroying the data of other users		P			P	P	P	P	P
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature		P	P	P			P	P	P
Continued infringements of the above, following previous warnings or sanctions		P	P		P	P	P	P	P
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school			P		P	P	P		P
Using proxy sites or other means to subvert the school's filtering system		P			P	P	P	P	P
Accidentally accessing offensive or pornographic		P			P	P		P	P

material and failing to report the incident									
Deliberately accessing or trying to access offensive or pornographic material		P	P	P	P	P	P	P	P
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act					P	P		P	P

Staff Actions / Sanctions

Incidents:	Refer to line managerr	Refer to Headteacher	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		P	P	P				
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email	P					P		
Unauthorised downloading or uploading of files	P					P		
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	P				P	P		
Careless use of personal data eg holding or transferring data in an insecure manner		P			P	P		
Deliberate actions to breach data protection or network security rules		P			P	P	P	
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		P	P	P				P
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature		P			P	P	P	P
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils	P	P			P	P		
Actions which could compromise the staff member's professional standing	P	P				P	P	P
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		P			P	P	P	P
Using proxy sites or other means to subvert the school's filtering system		P			P		P	
Accidentally accessing offensive or pornographic material and failing to report the incident	P				P			
Deliberately accessing or trying to access offensive or pornographic material		P			P	P	P	P
Breaching copyright or licensing regulations		P			P	P		
Continued infringements of the above, following previous warnings or sanctions		P	P				P	P