Cornerstone Multi Academy Trust

eSafety Policy

eSafety Practices
Teaching and Learning of eSafety

eSafety Practices

Introduction

Cornerstone Academy Trust creates and promotes a challenging learning environment that inspires children to achieve high standards and become life-long learners.

The Academy Trust has high expectations, builds children's confidence, and ensures success for all. We seek to foster creative thinkers, inquisitive questioners and avid problem solvers with flexible skills, who are successful communicators. Children learn to collaborate effectively at all levels, including working with our international partners and are able to adapt to the needs of a diverse and fast changing society.

New technologies play a valuable part in fulfilling the above. These 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. Significant educational benefits should result from curriculum internet use, including access to information from around the world and the ability to communicate widely. Internet safety depends on the Staff, the trust board, parents and carers to take responsibility for the use of the internet.

The internet is an essential element in 21st century life for education, business and social interaction. The School has a duty to provide children with quality internet access as part of their learning experience. The purpose of internet use in the School is to raise educational standards, to promote pupil achievement and to support the professional work of the Staff.

How pupils are protected from harm on the internet

- EYFS will only use nominated internet sites under close supervision.
- In KS1 pupils will access a wider range of sites, including search and self-guided, whilst under supervision.
- At KS2, pupils will be given a greater autonomy to use the internet, but under the specific guidance of teachers, and after they have shown they understand the principles of safe internet use
- The School will filter and monitor access to the internet for pupils
- Staff will exercise professional and reasonable precaution to ensure that pupils access only appropriate material
- Parents will be helped to understand how to keep children safe online

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 inappropriate contact including 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

- Downloading copyright material including music or video
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

This policy applies to all members of the school community (including staff, students / pupils, trustees, 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

Trustees:

The school governing body has a statutory responsibility for child protection and health and safety, and elements of these will include internet safety. 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 Trustees / Local Area Board; receiving regular information about e-safety incidents and monitoring reports. A member of the Governing Body (Ken Dyson) is the E-Safety Governor. The role of the E-Safety Governor will include:

- regular meetings with the E-Safety Co-ordinator
- regular monitoring of e-safety incident logs
- regular monitoring of filtering / change control logs
- reporting to relevant Governors committee / meeting

They should also be aware of the issues and risks of using ICT in the school, alongside the benefits, particularly with regard to the internet and other communications technologies. They should ensure that appropriate funding is authorised for internet safety solutions, training and other activities as recommended by the CEO, as part of the wider remit of the trust board with regard to school budgets.

Headteacher and Leadership Team:

- 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 CEO/ Heads of Schools and Senior Leaders are responsible for ensuring that the E-Safety Coordinator 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 / 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 Leadership team are aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.

E-Safety Co-ordinator

- 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
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments
- meets regularly with E-Safety trustee and team to discuss current issues, review incident logs and filtering / change control logs
- attends relevant meeting / committee of Governors
- reports regularly to Senior Leadership Team
- incidents will be dealt with in accordance to the school's disciplinary policy
- 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
- that users may only access the school's networks through a properly enforced password protection policy
    - Pupils are automatically assigned a password, that is normally two syllable with a two digit number at the end. They keep this password until it needs changing, such as if compromised
- the trust uses the SWGFL filtering system, lightspeed / smoothwall filtering solutions on all school devices, and eSafe filtering and key/screen logging software on all school windows devices.
- that the use of the network / office365 / remote access / email / Instant messaging / video conferencing is regularly monitored in order that any misuse / attempted misuse can be reported to the Leadership Team for investigation / action / sanction
- that monitoring software / systems are implemented and updated as agreed in trust policies

Teaching, Support Staff and Trustees:

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 trust Staff Acceptable Use Policy / Agreement (AUP)
- they report any suspected misuse or problem to the Leadership team for investigation / action / sanction
- digital communications with students / pupils (email / office365 / voice / social networking / public networks / instant messaging / video conferencing) should be on a professional level and only carried out using official school systems
- e-safety issues are embedded in all aspects of the curriculum and other school activities
- students / pupils understand and follow the school e-safety and acceptable use policy
- students / pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor ICT activity in lessons, extra-curricular and extended school activities
- they are aware of e-safety issues related to the use of mobile phones, cameras and handheld 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 / 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

Designated Person for Safeguarding

Will 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 Group

Members of the E-safety Group will assist the E-Safety lead / Officer (or another relevant person, as above) with:

- the production / review / monitoring of the school e-safety policy / documents.
- the production / review / monitoring of the school filtering policy (if the school chooses to have one) and requests for filtering changes.
- mapping and reviewing the e-safety curricular provision – ensuring relevance, breadth and progression
- monitoring network / internet / incident logs
- consulting stakeholders – including parents / carers and the students / pupils about the e-safety provision
- monitoring improvement actions identified through use of the 360-degree safe self-review tool

Pupils

- are responsible for using the school ICT systems in accordance with the Student / Pupil Acceptable Use Policy, which they sign as part of learning that they are responsible for what they do on a computer and online. (note - at EYFS/KS1 it would be expected that parents / carers would sign on behalf of the pupils)
- have a developing understanding of research skills and appreciate the need to avoid plagiarism by always showing when you have quoted someone else's work.
- 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 policy on the use of mobile phones, digital cameras and handheld 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

Teaching and Learning of eSafety

Whilst regulation and technical solutions are very important, their use must be balanced by educating students / pupils to take a responsible approach. The education of students / pupils in e-safety is therefore an essential part of the school's e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience.
E-Safety education will be provided in the following ways:

- A planned e-safety programme will be delivered as part of their education and will be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school
- The trust approach uses the progressive planning provided by South West Grid For Learning, in conjunction with the CEOP 'ThinkYouKnow' resources and Childline material.
- 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 / pupils should be helped to understand the need for the student / pupil AUP and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school
- Staff should act as good role models in their use of ICT, the internet and mobile devices
- In lessons where internet use is pre-planned, it is best practice that students / 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 can freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

Parents and 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. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website / VLE and information about national / local e-safety campaigns / 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 events
- access to parents' sections of the website and on-line student / pupil records
- their children's personal devices in the school (where this is allowed)

Parents and carers will be responsible for:

- endorsing (by signature) the Pupil Acceptable Use Policy
- accessing the school website / on-line pupil records systems in accordance with the relevant school Acceptable Use Policy.

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:

- Curriculum activities
- Letters, newsletters, web site, Office365
- Parents evenings
- Adult learning courses
- High profile events / campaigns e.g. Safer Internet Day
- Reference to the SWGfL Safe website (nb the SWGfL "Golden Rules" for parents)

The school will offer family learning courses in ICT, media literacy and e-safety so that parents and children can together gain a better understanding of these issues. Messages to the public around e safety should also be targeted towards grandparents and other relatives as well as parents. Everyone has a role to play in empowering children to stay safe while they enjoy these new technologies, just as it is everyone's responsibility to keep children safe in the non-digital world.

Staff/Volunteers

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:

- Regular sessions of formal e-safety training will be made available to staff. An audit of the e-safety training needs of all staff will be carried out regularly. It is expected that some staff will 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 provide advice / guidance / training as required to individuals as required.

Trustees and Local Area Board

Trustees should take part in e-safety training / awareness sessions, with particular importance for those who are members of any sub-committee / group involved in technology / e-safety / health and safety / child protection. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority / National Governors Association / or other relevant organisation (e.g. SWGfL).
- Participation in school training / information sessions for staff or parents (this may include attendance at the assemblies / lessons).

Curriculum

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages in the use of ICT across the curriculum.

When using digital images, staff should inform and educate students / 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.

- Staff are allowed to take digital / video images to support educational aims, but must follow school procedures 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. Staff must not share / distribute any images unless consent has been given by parents and the leadership team.
- Care should be taken when taking digital / video images to ensure that the school is not led into disrepute.
- Students' / Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.

- Written permission from parents or carers will be obtained before photographs of students / pupils are published on the school website

Data Protection

Personal data is any information that, when combined with other information, could be used to identify an individual ("natural born person"). This brings a wide range of information within the scope of what is considered personal data.

This includes clear personal data, such as:

- Name
- Address
- Date of birth
- Email address
- Login details

But also data such as:

- Test scores (as this could be combined with other data to identify an individual)
- Car number plates

Extra precautions must be taken with special category data, such as:

- Medical or health information
- Race or ethnic origin
- Religion or politics

Data which could refer to a group of 5 or less is generally considered personal data.

Whenever personal data is collected, processed, stored, or destroyed, this must be in compliance with the General Data Protection Regulation (GDPR)

All personal data must be for a specific purpose, and have a lawful basis for processing, in line with the school's data policies.

All staff must ensure that they take the utmost care to protect personal data, and to ensure that pupils do the same.

Protection for this data includes:

- Only holding it in ways approved in the trust's data retention policy
- Following good security practice by always locking workstations, using a secure password
- Not transferring the data in insecure ways

In the event that any member of staff believes that personal data has, or might have been, handled or disclosed in a way outside of the data retention policy they MUST inform the data protection officer (Graham Newbery) immediately. Data breaches may have to be notified to the information commissioner within 72 hours of discovery, so time is of the essence.

Social Media - Protecting Professional Identity

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

The *school's / academy's* use of social media for professional purposes will be checked regularly by the senior risk officer and e-safety committee to ensure compliance with the Social Media, Data Protection, Communications, Digital Image and Video Policies.

Unsuitable / inappropriate 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					ü
	promotion or conduct of illegal acts, e.g. under the child protection, obscenity, computer misuse and fraud legislation					ü
	adult material that potentially breaches the Obscene Publications Act in the UK					ü
	criminally racist material in UK					ü
	pornography				ü	
	promotion of any kind of discrimination				ü	
	promotion of racial or religious hatred				ü	
	threatening behaviour, including promotion of physical violence or mental harm				ü	
	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				ü	
Using school systems to run a private business					ü	
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by SWGfL and / or the school					ü	
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions					ü	
Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)					ü	

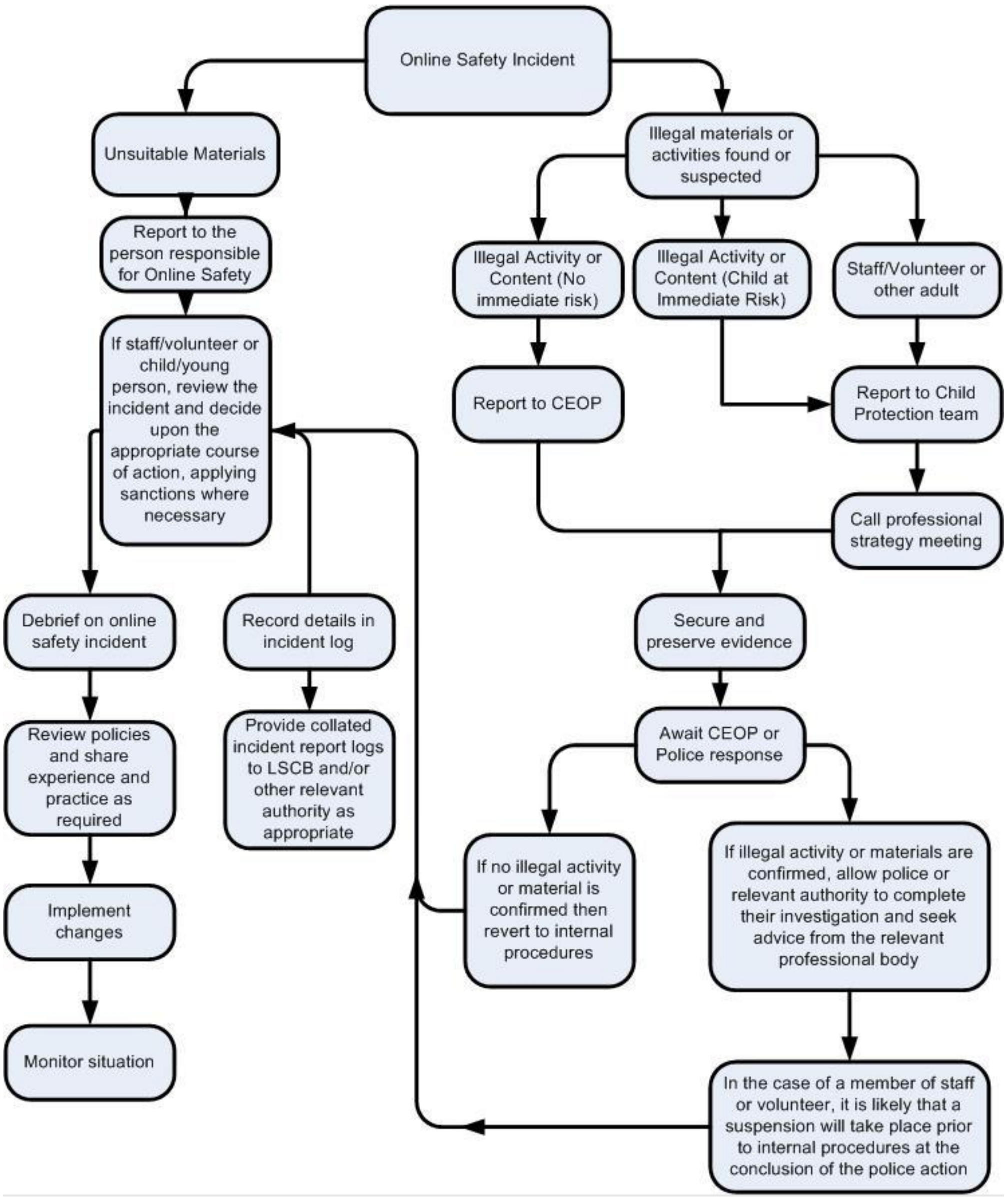
Creating or propagating computer viruses or other harmful files				ü	
Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet				ü	
On-line gaming (educational)		ü			
On-line gaming (non educational)				ü	
On-line gambling				ü	
On-line shopping / commerce		ü			
File sharing				ü	
Use of social networking sites			ü		
Use of video broadcasting e.g. YouTube			ü		

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, i.e.:

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

refer to the right-hand side of the Flowchart for responding to online safety incidents and report immediately to the police.

The SWGfL flow chart – below and http://www.swgfl.org.uk/safety/default.asp should be consulted and actions followed in line with the flow chart, in particular the sections on reporting the incident to the police and the preservation of evidence.


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

Other Incidents

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

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

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).

- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)

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

    - Internal response or discipline procedures
    - Involvement by Local Authority or national / local organisation (as relevant).
    - Police involvement and/or action
    - If content being reviewed includes images of Child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:
    - incidents of 'grooming' behaviour
    - the sending of obscene materials to a child
    - adult material which potentially breaches the Obscene Publications Act
    - criminally racist material
    - Other criminal conduct, activity or materials
    - Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

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

School Actions

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:

Pupils **Actions**

Incidents:	Refer to class teacher / tutor	Refer to Leadership Team	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering /	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction e.g. detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).			ü	ü					
Unauthorised use of non-educational sites during lessons	ü								
Unauthorised use of mobile phone / digital camera / other handheld device	ü				ü				
Unauthorised use of social networking / instant messaging / personal email	ü								
Unauthorised downloading or uploading of files	ü								
Allowing others to access school network by sharing username and passwords		ü							
Attempting to access or accessing the school network, using another student's / pupil's account	ü								
Attempting to access or accessing the school network, using the account of a member of staff		ü	ü			ü			
Corrupting or destroying the data of other users	ü								
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature		ü							
Continued infringements of the above, following previous warnings or sanctions		ü							

Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		ü							
Using proxy sites or other means to subvert the school's filtering system		ü			ü				
Accidentally accessing offensive or pornographic material and failing to report the incident		ü	ü		ü	ü			
Deliberately accessing or trying to access offensive or pornographic material		ü	ü	ü			ü	ü	
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act		ü							

Staff **Actions**

Incidents:	Refer to Leadership	Refer to ISP	Refer to Police	Refer to Technical Support Staff for action re filtering etc.	Warning	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	ü	ü	ü	ü		ü
Inappropriate personal use of the internet / social networking sites / instant messaging / personal email	ü				ü	
Unauthorised downloading or uploading of files	ü					
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	ü				ü	

Careless use of personal data e.g. holding or transferring data in an insecure manner	ü					
Deliberate actions to breach data protection or network security rules	ü	ü				
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	ü	ü				ü
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	ü	ü				ü
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils not connected to education	ü			ü		ü
Actions which could compromise the staff member's professional standing	ü				ü	
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	ü				ü	
Using proxy sites or other means to subvert the school's filtering system	ü					
Accidentally accessing offensive or pornographic material and failing to report the incident	ü			ü		
Deliberately accessing or trying to access offensive or pornographic material	ü					ü
Breaching copyright or licensing regulations	ü				ü	
Continued infringements of the above, following previous warnings or sanctions	ü					ü