Al Islah Girls' High School

E-Safety Policy

Online Safety School Policy

Development / Monitoring / Review of this Policy

This e-safety policy has been developed by a working group made up of:

- Headteacher
- School appointed E-Safety Officer
- Staff – including Teachers, Support Staff, Technical staff
- E-Safety Lead Governor

Schedule for Development / Monitoring / Review

This e-safety policy was approved by the Board of Directors /Governing Body / Governors Sub Committee on:	May 2017
The implementation of this e-safety policy will be monitored by the:	Head teacher School appointed E-Safety Officer E-Safety Lead Governor DSL
Monitoring will take place at regular intervals:	Annually
The Governing Body 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:	Quarterly
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:	DSL, MASH Team, E-Safety Lead Governor and the Police (depending on level of incident)

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 activity

Scope of the Policy

This policy to all staff including the governing body, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for or provide services on behalf of the school (collectively referred to as 'staff' in this policy) as well as children and parents/carers.

The Education and Inspections Act 2006 empowers Headteacher to such extent as is reasonable, to regulate the behaviour of students 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 outside of the schoolbut is linked to membership of the school / academy. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data.

In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

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 e-safety roles and responsibilities of individuals and groups within the school.

Governors / Board of Directors:

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 receiving regular information about e-safety incidents and monitoring reports. A member of the Governing Body has taken on the role of E-Safety Governor (Yusuf Patel).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

Ensuring there are appropriate and up-to-date policies and procedures regarding online safety.

Ensure that appropriate risk assessments are undertaken regarding the safe use of technology, including ensuring the safe and responsible use of devices.

Headteacher / Principal and Senior Leaders:

- **The Headteacher has a duty of care for ensuring the safety (including e-safety) of members of the school community**. The headteacher will also take on the role of E-Safety coordinator along with the DSL.
- **The Headteacher and the Office Manager are aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.** (see flow chart on dealing with e-safety incidents – included in a later section – "Responding to incidents of misuse" and relevant Local Authority HR / other relevant body disciplinary procedures).
- The Headteacher is responsible for ensuring that the E-Safety Coordinator / Officer and other relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.
- The Headteacher 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

E-Safety Coordinator / Officer:

- 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

- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments)

  Maintaining an online safety incident/action log to record incidents and actions taken as part of the schools safeguarding recording structures and mechanisms. This will be in the safeguarding and child protection folders.
- meets regularly with E-Safety Governor to discuss current issues, review incident logs and filtering / change control logs
- attends relevant meeting / committee of Governors
- Coordinating participation in local and national events to promote positive online behaviour, e.g. Safer Internet Day.
- Liaising with the local authority and other local and national bodies as appropriate.
- Ensuring that online safety is integrated with other appropriate school policies and procedures.

Network Manager / Technical staff:

The Network Manager is responsible for ensuring:

- **that the school's technical infrastructure is safe andsecure and is not open to misuse or malicious attack**
- **that the school meets required e-safety technical requirements and any Local Authority / other relevant body E-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**
- the filtering policy is applied and updated on a regular basis and passwords are changed quarterly. Its implementation is not the sole responsibility of any single person
- that they keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant
- that the use of the network is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher and E-Safety Coordinator for investigation and recorded on the E-Safety incident log
- that monitoring software / systems are implemented and updated as agreed in school policies

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 / academy e-safety policy and practices**
- **they have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP)**
- **they report any suspected misuse or problem to the Headteacher and E Safety coordinator**
- **all digital communications with students / pupils / parents / carers 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 activities
- students understand and follow the e-safety and acceptable use policies
- students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current 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

- Embedding online safety education in curriculum delivery wherever possible.

Child Protection / Safeguarding Designated Person / Officer

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

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

Students / pupils:

- **are responsible for using the school / academydigital technology systems in accordance with the Student / 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 policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying.
- should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's / academy'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 / academy will take every opportunity to help parents understand these issues through newsletters, letters and the school website. 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
- Seeking help and support from the School, or other appropriate agencies, if they or their child encounters online problems or concerns.

Policy Statements

Education – students / pupils

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.

Online Safety School Policy

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages across the curriculum. The e-safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- **A planned e-safety curriculum should be provided as part of ICT lessons and should be regularly revisited**
- **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 taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet**
- Students / pupils should be helped to understand the need for the student / 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 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 students / pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

Education – parents / carers

Many parents and carers have only a limited understanding of 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 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
- Parents / Carers evenings / sessions
- High profile events / campaigns eg Safer Internet Day

Education & Training – 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:

- **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 Agreements.**
- The E-Safety Coordinator / Officer (or other nominated person) will receive regular updates through attendance at external training events (eg from SWGfL / LA / other relevant organisations) and by reviewing guidance documents released by relevant organisations.
- This E-Safety policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.
- The E-Safety Coordinator / Officer (or other nominated person) will provide advice / guidance / training to individuals as required.

Training – Governors / Directors

Governors / Directors 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:

- Participation in school training / information sessions for staff or parents(this may include attendance at assemblies / lessons).

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 / Academy technical systems will be managed in ways that ensure that the school / academy meets recommended technical requirements**
- **There will be regular reviews and audits of the safety and security of school academy technical systems**
- **Servers, wireless systems and cabling must be securely located and physical access restricted**
- **All users will have clearly defined access rights to school / academy technical systems and devices.**
- **All userswill be provided with a username and secure password** by Yusuf Patel who will keep an up to date record of users and their usernames.**Users are responsible for the security of their username and password**and will be required to change their password every three months
- **The "master / administrator" passwords for the school / academy ICT system, used by the Network Manager (or other person) must also be available to the Headteacher or other nominated senior leader and kept in a secure place**
- Yusuf Patel **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 installation**
  - **Internet access is filtered for all users.** Illegal content (child sexual abuse images, including extremist material) is filtered by the broadband or filtering provider by Smoothwall filtering system
- • The school has provided differentiated user-level filtering
- School / academy technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.
- An appropriate system is in placefor users to report any actual / potential technical incident / security breach to the relevant person, as agreed).
- Appropriate security measures are in place (schools may wish to provide more detail) to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- An agreed policy is in placethat allows staff forbids staff from downloading executable files and installing programmes on school devices.
- An agreed policy is in placeregarding the use of removable media by users on school devices.Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.Staff are not able to use removable media (USB, CD) on the school network.

Bring Your Own Device (BYOD)

Staff are able to bring in their own laptops. However, they must ensure that:

- Internet is used through the school network to ensure the filtering system will work

- Mobile phones are not allowed to be connected to the WiFi system
- Personal USB sticks must not be used

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 and access for users is differentiated
- 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
- Mandatory training is undertaken for all staff
- Students/Pupils receive training and guidance on the use of personal devices
- Regular audits and monitoring of usage will take place to ensure compliance

When using communication technologies the school considers the following as good practice:

- **The official school / academy email service may be regarded as safe and secure and is monitored.Users should be aware that email communications are monitored.** Staff and students / pupils should therefore use only the school / academy email service to communicate with others when in school, or on school / academy systems (eg by remote access).
- **Users must immediately report, to the nominated person – in accordance with the school / academy policy, 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 students / pupils or parents / carers (email, chat, VLE etc) must be professional in tone and content.**These communications may only take place on official (monitored) school / academy systems. Personal email addresses, text messaging or social media must not be used for these communications.
- School email addresses and other official contact details will not be used for setting up personal social media accounts.
- Students / pupils should be taught about e-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 / academy website and only official email addresses should be used to identify members of staff.

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
- Personal opinions should not be attributed to the school /academy

- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.
- All members of the School community are advised not to publish specific and detailed private thoughts, concerns, pictures or messages on any social media services, especially content that may be considered threatening, hurtful or defamatory to others.
- The use of social networking applications during school hours for personal use is/is not permitted.
- Official use of social media sites as communication tools will be risk assessed and formally approved by the headteacher.
- Staff will use school provided email addresses to register for and manage official school approved social media channels.
- Parents/Carers and students will be informed of any official school social media use, along with expectations for safe use

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.

Use of Personal Devices and Mobile Phones

Please see Mobile Phone Policy

Responding to concerns regarding Self-Generated Indecent Images of Children (SGIIOC or "Sexting")

Please see sexting policy

Responding to concerns regarding radicalisation or extremism online, Online Child Sexual Abuse, Indecent Images of Children and cyberbullying

Concerns regarding students must be passed on to the DSL using a cause for concern form. If the issue in question is of a severe nature, staff must see the DSL in person to report this.

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 usage as follows:

Online Safety School Policy

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 –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	pornography				X	
	promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	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				X	
Using school systems to run a private business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / academy					X	
Infringing copyright					X	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)					X	
Creating or propagating computer viruses or other harmful files					X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)					X	
On-line gaming (educational)				X		
On-line gaming (non educational)					X	
On-line gambling					X	
On-line shopping / commerce					X	
File sharing				X		
Use of social media					x	
Use of messaging apps					x	
Use of video broadcasting eg Youtube				x		

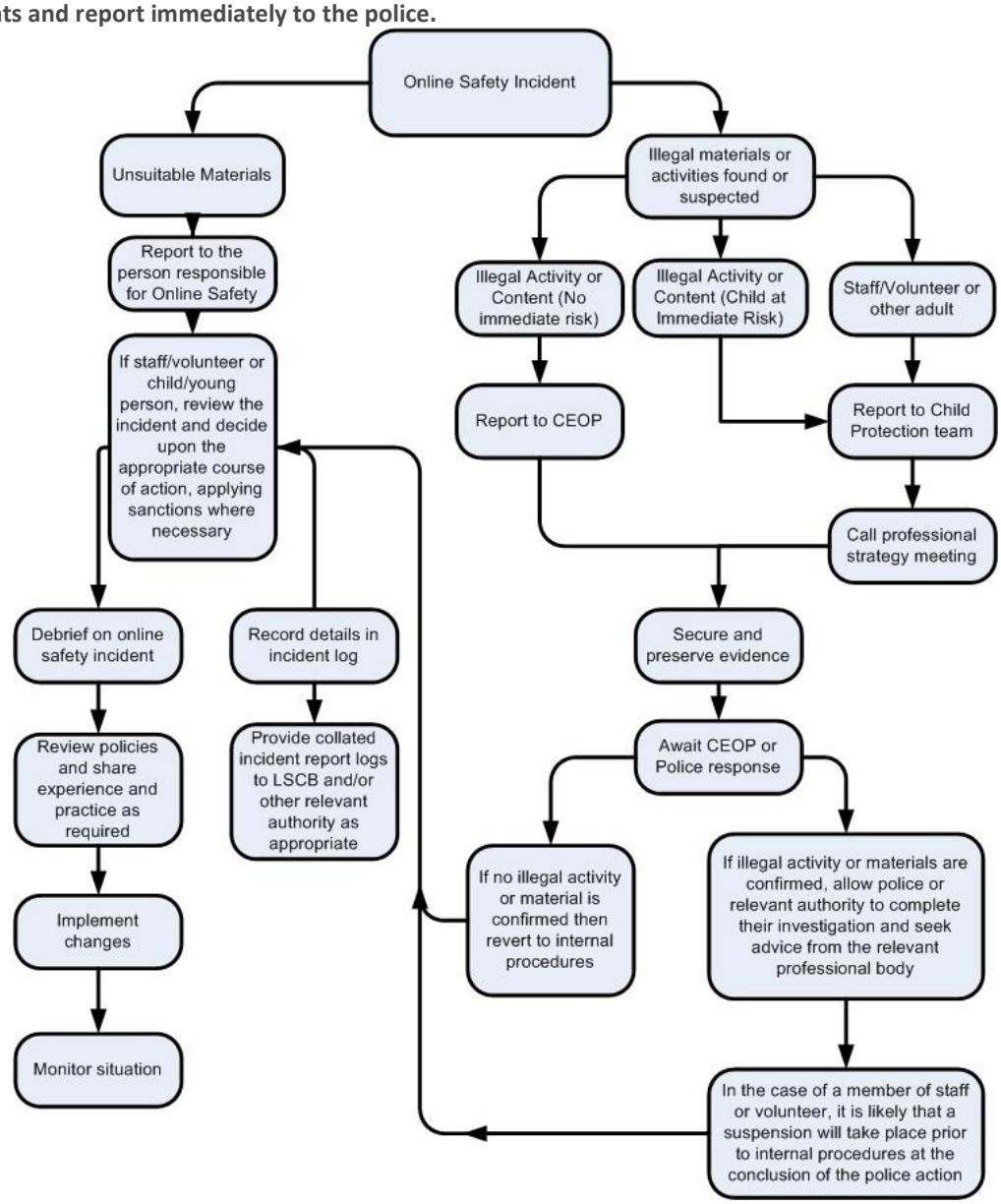
Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities.

Online Safety School Policy

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the police.



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 / volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.

- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the url of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
    - Internal response or discipline procedures
    - Involvement by Local Authority or national / local organisation (as relevant).
    - Police involvement and/or action
- **If content being reviewed includes images of Child abusethen 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 / Academy Actions & Sanctions

It is more likely that the school / academy 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 / Pupils Actions / Sanctions

Incidents:	Refer to class teacher / tutor	Refer to Head of Department / Head of Year / other	Refer to Headteacher / Principal	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).			X	X		X			
Unauthorised use of non-educational sites during lessons	X								
Unauthorised use of mobile phone / digital camera / other mobile device	X							X	
Unauthorised use of social media / messaging apps / personal email	X							X	

Unauthorised downloading or uploading of files			X					X	
Allowing others to access school / academy network by sharing username and passwords			X					X	
Attempting to access or accessing the school / academy network, using another student's / pupil's account	X							X	
Attempting to access or accessing the school / academy network, using the account of a member of staff			X			X			X
Corrupting or destroying the data of other users			X			X			X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature			X			X			X
Continued infringements of the above, following previous warnings or sanctions			X			X	X		X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school			X			X	X		X
Using proxy sites or other means to subvert the school's / academy's filtering system			X		X	X	X		X
Accidentally accessing offensive or pornographic material and failing to report the incident (depending on level, police will be informed)			X	X	X	X	X		X
Deliberately accessing or trying to access offensive or pornographic material (depending on level, police will be informed)			X	X	X	X	X		X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act			X	X	X	X	X		X

Staff Actions / Sanctions

Incidents:	Refer to line managerr	Refer to Headteacher Principal	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).		X	X	X				X
Inappropriate personal use of the internet / social media / personal email		X			X	X		
Unauthorised downloading or uploading of files		X			X			
Allowing others to access school network by sharing username and passwords or attempting to access or		X			X	X		X

accessing the school network, using another person's account								
Careless use of personal data eg holding or transferring data in an insecure manner		X			X	X		X
Deliberate actions to breach data protection or network security rules		X			X	X		
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		X			X	X		X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		X				X		X
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils		X		X		X		X
Actions which could compromise the staff member's professional standing		X						
Actions which could bring the school / academy into disrepute or breach the integrity of the ethos of the school / academy		X				X		X
Using proxy sites or other means to subvert the school's / academy's filtering system		X			X	X		X
Accidentally accessing offensive or pornographic material and failing to report the incident		X			X	X		X
Deliberately accessing or trying to access offensive or pornographic material		X		X		X		X
Breaching copyright or licensing regulations		X			X	X		X
Continued infringements of the above, following previous warnings or sanctions		X			X	X		X