eSafety
Policy

Last review date::	October 2017
Scheduled review date:	October 2019

Oak Academy – eSafety Policy

1.0 Scope of the Policy

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

The Education and Inspections Act 2006 empowers Principals to such extent as is reasonable, to regulate the behaviour of students when they are off the academy site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other eSafety incidents covered by this policy, which may take place outside of the academy, but is linked to membership of the 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 academy 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 eSafety behaviour that take place out of school.

2.0 Roles and Responsibilities

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

2.1 Governors:

Governors are responsible for the approval of the eSafety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about eSafety incidents and monitoring reports. A member of the Governing Body has taken on the role of eSafety Governor. The role of the eSafety Governor will include:

- regular meetings with the eSafety Co-ordinator / Officer
- regular monitoring of eSafety incident logs
- regular monitoring of filtering / change control logs
- reporting to relevant Governors / Board / committee / meeting

2.2 Principal and Senior Leaders:

- The Principal has a duty of care for ensuring the safety (including eSafety) of members of the school community, though the day-to-day responsibility for eSafety will be delegated to the eSafety Co-ordinator/Designated Safeguard Lead (DSL).

- The Principal and (at least) another member of the Senior Leadership 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. (see flow chart on dealing with eSafety incidents – included in a later section – "Responding to incidents of misuse" and relevant Local Authority HR / other relevant body disciplinary procedures).
- The Principal / Senior Leaders are responsible for ensuring that the eSafety Coordinator/DSL and other relevant staff receive suitable training to enable them to carry out their eSafety roles and to train other colleagues, as relevant.
- The Principal/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 eSafety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Senior Leadership Team will receive regular monitoring reports from the eSafety Co-ordinator/DSL.

2.3 eSafety Coordinator / DSL:

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

2.4 Network Manager / Technical staff:

The Network Manager/Technical Staff is responsible for ensuring:

- **that the academy's technical infrastructure is secure and is not open to misuse or malicious attack**
- **that the academy meets required eSafety technical requirements and any Local Authority eSafety Policy 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 that its implementation is not the sole responsibility of any single person (see appendix "Technical Security Policy Template" for good practice)

- that they keep up to date with eSafety technical information in order to effectively carry out their eSafety role and to inform and update others as relevant
- that the use of the network/internet/remote access/email is regularly monitored in order that any misuse/attempted misuse can be reported to the Principal/Senior Leader; eSafety Coordinator/DSL for investigation/action/sanction
- that monitoring software/systems are implemented and updated as agreed in academy policies

2.4 Teaching and Support Staff

are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current academy eSafety policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy (AUP)
- they report any suspected misuse or problem to the Principal/Senior Leader; eSafety Coordinator/DSL for investigation/action/sanction
- all digital communications with students/parents/carers should be on a professional level and only carried out using official school systems
- eSafety issues are embedded in all aspects of the curriculum and other activities
- students understand and follow the eSafety 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*

2.5 Designated Safeguard Lead/eSafety Coordinator

Should be trained in eSafety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

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

2.6 Students / pupils

- are responsible for using the academy digital technology systems in accordance with the Student 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 eSafety practice when using digital technologies out of school and realise that the academy's eSafety Policy covers their actions out of school, if related to their membership of the school

2.7 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 academy will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website/VLE and information about national/local eSafety campaigns/literature. Parents and carers will be encouraged to support the academy in promoting good eSafety 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/VLE and online student records
- their children's personal devices in the academy (where this is allowed)

2.8 Community Users

Community Users who access school systems/website/VLE as part of the wider academy provision will be expected to sign a Community User AUA before being provided with access to school systems. (A Community Users Acceptable Use Agreement Template can be found in the appendices.)

3.0 Policy Statements

3.1 Education – students

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 pupils in eSafety is therefore an essential part of the school's eSafety provision. Children and young people need the help and support of the school to recognise and avoid eSafety risks and build their resilience.

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

- A planned eSafety curriculum should be provided as part of Computing/SMSC/other lessons and should be regularly revisited
- Key eSafety messages should be reinforced as part of a planned programme of assemblies and tutorial/pastoral activities
- Students should be taught in all lessons to be critically aware of the materials/content they access online and be guided to validate the accuracy of information.
- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Students should be helped to understand the need for the student Acceptable Use Policy 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 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 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.

3.2 Education – parents/carers

Many parents and carers have only a limited understanding of eSafety risks and issues, yet they play an essential role in the education of their children and in the monitoring/regulation of the children's online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and carers through: (select / delete as appropriate)

- Curriculum activities
- Letters, newsletters, website, VLE
- Parents/Carers evenings/sessions
- High profile events/campaigns e.g. Safer Internet Day
- Reference to the relevant web sites/publications e.g. www.swgfl.org.uk www.saferinternet.org.uk/http://www.childnet.com/parents-and-carers (see appendix for further links / resources)

3.3 Education – The Wider Community

The academy will provide opportunities for local community groups/members of the community to gain from the academy's eSafety knowledge and experience. This may be offered through the following:

- Providing family learning courses in use of new digital technologies, digital literacy and e-safety
- ESafety messages targeted towards grandparents and other relatives as well as parents.
- The school / academy website will provide e-safety information for the wider community
- Supporting community groups eg Early Years Settings, Childminders, youth/sports /voluntary groups to enhance their eSafety provision (possibly supporting the group in the use of Online Compass, an online safety self review tool - www.onlinecompass.org.uk)

3.4 Education & Training – Staff / Volunteers

It is essential that all staff receive eSafety 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. This will be regularly updated and reinforced. 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 eSafety training as part of their induction programme, ensuring that they fully understand the school eSafety policy and Acceptable Use Policy.
- The eSafety Coordinator/DSL (or other nominated person) will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.
- This eSafety policy and its updates will be presented to and discussed by staff in staff/team meetings/INSET days.
- The eSafety Coordinator/DSL(or other nominated person) will provide advice/guidance/training to individuals as required.

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

3.6 Technical – infrastructure/equipment, filtering and monitoring

The academy 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 eSafety responsibilities:

- Academy technical systems will be managed in ways that ensure that the 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 academy technical systems and devices.
- All users will be provided with a username and secure password by the Network Manager 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 12 months.
- The administrator passwords for the academy ICT system, used by the Network Manager must also be available to the Principal or other nominated senior leader and kept in a secure place (eg school safe)
- The 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 sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes (see appendix for more details)
- The school has provided enhanced/differentiated user-level filtering (allowing different filtering levels for different ages/stages and different groups of users – staff/students etc)
- 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 Policy.
- An appropriate system is in place for users to report any actual/potential technical incident/security breach to the relevant person, as agreed.
- 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 virus software.

- An agreed policy is in place for the provision of temporary access of "guests" (eg trainee teachers, supply teachers, visitors) onto the school systems.
- An agreed policy is in place regarding the extent of personal use that users (staff/students/community users) and their family members are allowed on school devices that may be used out of school.
- An agreed policy is in place that allows staff to / forbids staff from downloading executable files and installing programmes on school devices.
- An agreed policy is in place regarding the use of removable media (eg memory sticks / CDs / DVDs) 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. (see School Personal Data Policy Template in the appendix for further detail)

4.0 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 eSafety 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. This list is not exhaustive and a BYOD policy should be in place and reference made within all relevant policies.

- The school has a set of clear expectations and responsibilities for all users
- The school adheres to the Data Protection Act & GDPR principles/regulations
- All users are provided with and accept the Acceptable Use Policy
- All network systems are secure and access for users is differentiated
- Where possible these devices will be covered by the 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 receive training and guidance on the use of personal devices
- Regular audits and monitoring of usage will take place to ensure compliance
- Any device loss, theft, change of ownership of the device will be reported as in the BYOD policy
- Any user leaving the school will follow the process outlined within the BYOD policy

5.0 Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and students need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate 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.
- In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other students in the digital/video images.
- Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital/video images that 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.

6.0 Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 and is fully GDPR compliant

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 policies 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.

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.
- Transfer data using encryption and secure password protected devices.

When personal data is stored on any portable computer system, memory stick or any other removable media:

- the data must be encrypted and password protected
- the device must be password protected (many memory sticks / cards and other mobile devices cannot be password protected)
- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete

7.0 Communications

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

	Staff & other adults			Students				
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times/areas	Allowed with staff permission	Not allowed
Mobile phones may be brought to school	X					X		
Use of mobile phones in lessons			X				X	
Use of mobile phones in social time		X				X		
Taking photos on mobile phones / cameras		X					X	
Use of other mobile devices eg tablets, gaming devices		X					X	
Use of personal email addresses in school, or on school network			X					X
Use of school email for personal emails			X					X
Use of messaging apps		X				X		
Use of social media		X				X		
Use of blogs		X				X		

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

- The official 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 should therefore use only the academy email service to communicate with others when in school, or on academy systems (eg by remote access).

- Users must immediately report, to the nominated person – in accordance with the 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 or parents/carers (email, chat, VLE etc) must be professional in tone and content. These communications may only take place on official (monitored) academy systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Students should be taught about eSafety 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 academy website and only official email addresses should be used to identify members of staff.

7.1 Social Media

- All Social Media falls under the responsibility of one central accountable individual, this will be the Principal or a single designated member of staff appointed by the Principal.
- There should be no other social media interactions on a whole academy basis.
- If it is to support learning, curriculum areas may wish to share learning resources via a Twitter account. However, these interactions must be known to the Principal or single designated member of staff appointed by the Principal. Content and comments must only relate to appropriate curriculum learning.
- Teachers can only use Twitter for academic Academy purposes
- Use of closed communication channels, such as WhatsApp, are not permitted.

All schools, academies and local authorities have a duty of care to provide a safe learning environment for students and staff. 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 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, 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.

8.0 Unsuitable / inappropriate activities

The academy believes that the activities referred to in the following section would be inappropriate in a academy context and that users, as defined below, should not engage in these activities in academy or outside academy when using academy equipment or systems. The academy policy restricts usage as follows:

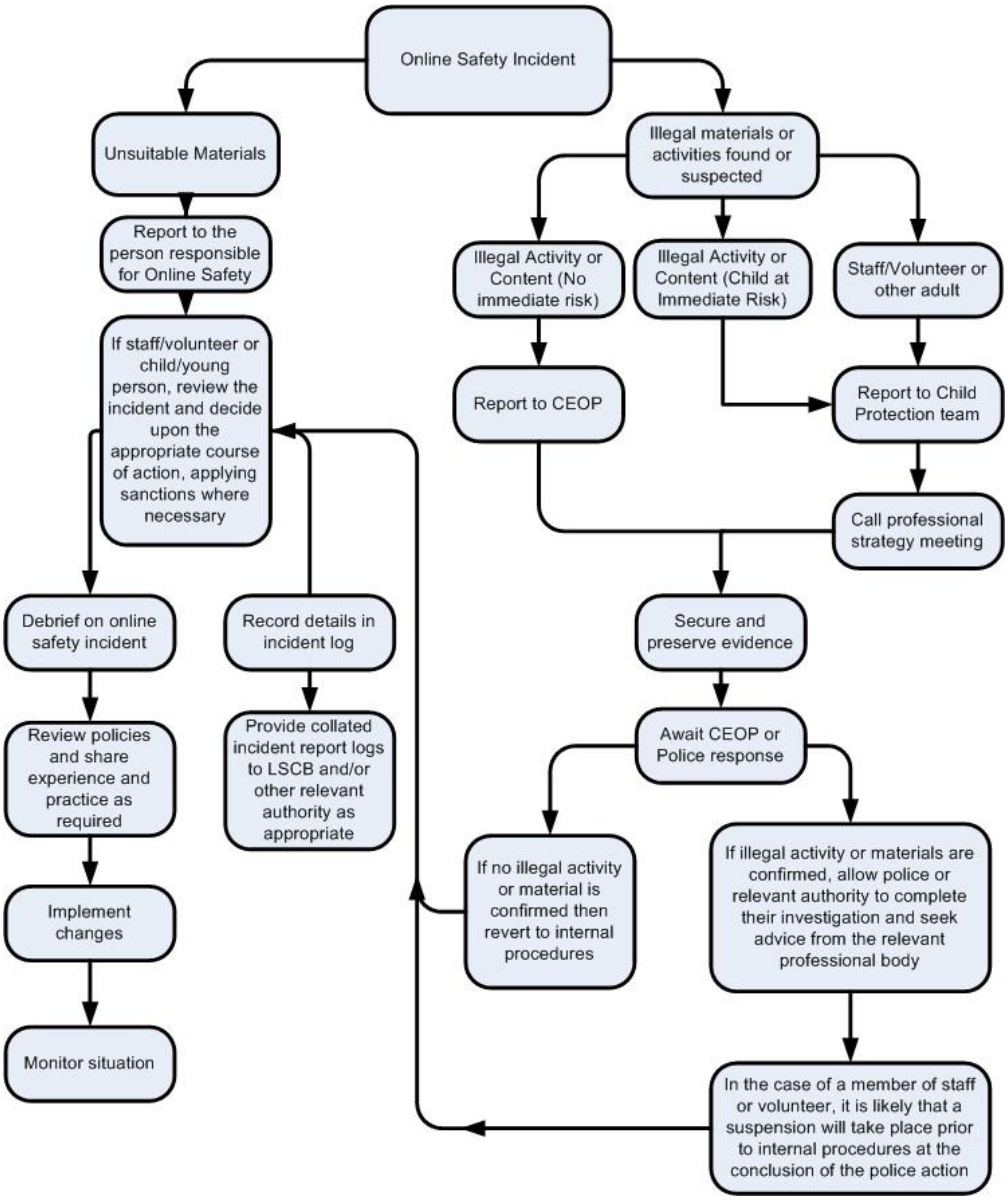
User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images –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			

9.0 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 (see "User Actions" above).

9.1 Illegal Incidents

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



9.2 Other Incidents

It is hoped that all members of the academy community will be responsible users of digital technologies, who understand and follow 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 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 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.

9.3 Academy Actions & Sanctions

It is more likely that the 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 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	X			X	X	X		
Unauthorised use of mobile phone / digital camera / other mobile device	X	X							
Unauthorised use of social media / messaging apps / personal email	X	X			X	X	X		
Unauthorised downloading or uploading of files	X	X			X	X	X		
Allowing others to access school / academy network by sharing username and passwords	X	X			X	X	X	X	
Attempting to access or accessing the school / academy network, using another student's / pupil's account	X	X						X	
Attempting to access or accessing the school / academy network, using the account of a member of staff	X	X			X	X	X		X
Corrupting or destroying the data of other users	X	X	X		X	X	X		X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	X				X	X		X
Continued infringements of the above, following previous warnings or sanctions	X	X				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	X	X	X	X
Using proxy sites or other means to subvert the school's / academy's filtering system	X	X			X	X	X	X	X
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X			X	X			X
Deliberately accessing or trying to access offensive or pornographic material	X	X	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	X	X	X

Staff Actions / Sanctions

Incidents:	Refer to line managerr	Refer to 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				
Inappropriate personal use of the internet / social media / personal email	X							
Unauthorised downloading or uploading of files	X							
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	X	X			X			
Careless use of personal data eg holding or transferring data in an insecure manner	X				X			
Deliberate actions to breach data protection or network security rules	X	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	X	X
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils	X	X				X	X	X
Actions which could compromise the staff member's professional standing		X				X	X	X
Actions which could bring the school / academy into disrepute or breach the integrity of the ethos of the school / academy		X				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	X	X
Deliberately accessing or trying to access offensive or pornographic material		X	X	X	X	X	X	X
Breaching copyright or licensing regulations		X			X	X	X	X
Continued infringements of the above, following previous warnings or sanctions		X			X	X	X	X

Acceptable Use Policy – Staff

Note. All internet and email activity is subject to monitoring

You must read this policy in conjunction with the eSafety policy. Once you have read and understood both you must sign this policy sheet.

Internet access – You must not access or attempt to access any sites that contain any of the following: child abuse; pornography; promoting discrimination of any kind; promoting racial or religious hatred; promoting illegal acts; any other information which may be illegal or offensive to colleagues. Inadvertent access must be treated as an e-safety incident, reported to the e-safety coordinator and an incident sheet completed. Use of internet should be for educational purposes only during timetabled hours. All personal use should be restricted to non-contact time only.

Social networking – is allowed in the federation in accordance with the eSafety policy only. Staff using social networking for personal use should never undermine the federation, its staff, parents or children. Staff should not become 'friends' with parents or pupils on personal social networks

Use of email – staff are not permitted to use the federation email addresses for personal business. All email should be kept professional. Staff are reminded that federation data, including emails, is open to Subject Access Requests under the Freedom of Information Act.

Passwords – Staff should keep passwords private. However, these passwords are often shared with IT support allowing diagnostics within the specific users logged on context. Passwords should be changed immediately afterwards.

Data protection – If it is necessary for you to take work home, or off site, you should ensure that your device (laptop, USB pendrive etc.) is encrypted. On no occasion should data concerning personal information be taken offsite on an unencrypted device. This includes safe use of the federation's home access software and e-portal – staff should ensure that they are fully logged out of them after use.

Personal use of federation ICT – You are not permitted to use ICT equipment for personal use unless specific permission has been given from the Executive Principal who will set boundaries of personal use.

Images and videos – You should not upload onto any internet site or service images or videos of yourself, other staff or pupils without consent. This is applicable professionally (in the federation) or personally (i.e. offsite outings)

Use of personal ICT – Personal ICT equipment is allowed to be connected to the academies wireless network to access internet based resources for staff and post 16. This facility is extended on the understanding that suitable virus and malware precautions are taken and that no attempts are made to connect unauthorised internet services. This connectivity is closely monitored. Use of personal ICT equipment is at the discretion of the Executive Principal. Permission must be sought stating the reason for using personal equipment; a risk assessment will be carried out by IT support and the e-safety coordinator.

Viruses and other malware – any virus outbreaks are to be reported to the IT helpdesk as soon as it is practical to do so, along with the name of the virus (if known) and actions taken by the federation.

E-safety – like health and safety, e-safety is the responsibility of everyone. As such you will promote positive e-safety messages in all use of ICT whether you are with other members or with students.

Name:

Signature:

Date:

Acceptable Use Policy – Students

Our Charter of Good Online Behaviour & Acceptable Use of Equipment

Note: All Internet and email activity is subject to monitoring

I Promise – to only use the school ICT for schoolwork that the teacher has asked me to do.

I Promise – not to look for or show other people things that may be upsetting.

I Promise – to show respect for the work that other people have done.

I will not – use other people's work or pictures without permission to do so.

I will not – share my password with anybody. If I forget my password I will let my teacher know.

I will not – use other people's usernames or passwords.

I will not – share personal information online with anyone.

I will not – download anything from the Internet unless my teacher has asked me to.

I will – let my teacher know if anybody asks me for personal information.

I will – let my teacher know if anybody says or does anything to me that is hurtful or upsets me.

I will – be respectful to everybody online ; I will treat everybody the way that I want to be treated.

I understand – misuse of the Academy computers will lead to the possible restriction of computer access and consequences as stated in the Behaviour for Learning Policy may be implemented up to and including permanent exclusion

I understand – any wilful damage caused to Academy equipment will be charged to my Parents / Carers and consequences as stated in the Behaviour for Learning Policy may be implemented up to and including permanent exclusion

I understand – that some people on the Internet are not who they say they are, and some people can be nasty. I will tell my teacher if I am ever concerned in school, or my parents if I am at home.

I understand – if I break the rules in this charter there will be consequences of my actions and my parents will be told.

Signed (Parent) :

Signed (Student) :

Date :

Please return to relevant Year Office

Acceptable Use Policy – KS4 & 5 Students

Our Charter of Good Online Behaviour & Acceptable Use of Equipment

Note: All Internet and email activity is subject to monitoring

I Promise – to only use the school ICT for schoolwork that the teacher has asked me to do.

I Promise – not to look for or show other people things that may be upsetting.

I Promise – to show respect for the work that other people have done.

I will not – use other people's work or pictures without permission to do so.

I will not – share my password with anybody. If I forget my password I will let my teacher know.

I will not – use other people's usernames or passwords.

I will not – share personal information online with anyone.

I will not – download anything from the Internet unless my teacher has asked me to.

I will – let my teacher know if anybody asks me for personal information.

I will – let my teacher know if anybody says or does anything to me that is hurtful or upsets me.

I will – be respectful to everybody online ; I will treat everybody the way that I want to be treated.

I understand – misuse of the Academy computers will lead to the possible restriction of computer access and consequences as stated in the Behaviour for Learning Policy may be implemented up to and including permanent exclusion

I understand – any wilful damage caused to Academy equipment will be charged to my Parents / Carers and consequences as stated in the Behaviour for Learning Policy may be implemented up to and including permanent exclusion

I understand – that some people on the Internet are not who they say they are, and some people can be nasty. I will tell my teacher if I am ever concerned in school, or my parents if I am at home.

I understand – if I break the rules in this charter there will be consequences of my actions and my parents will be told.

Signed (Student) :

Date :

Please return to relevant Year Office