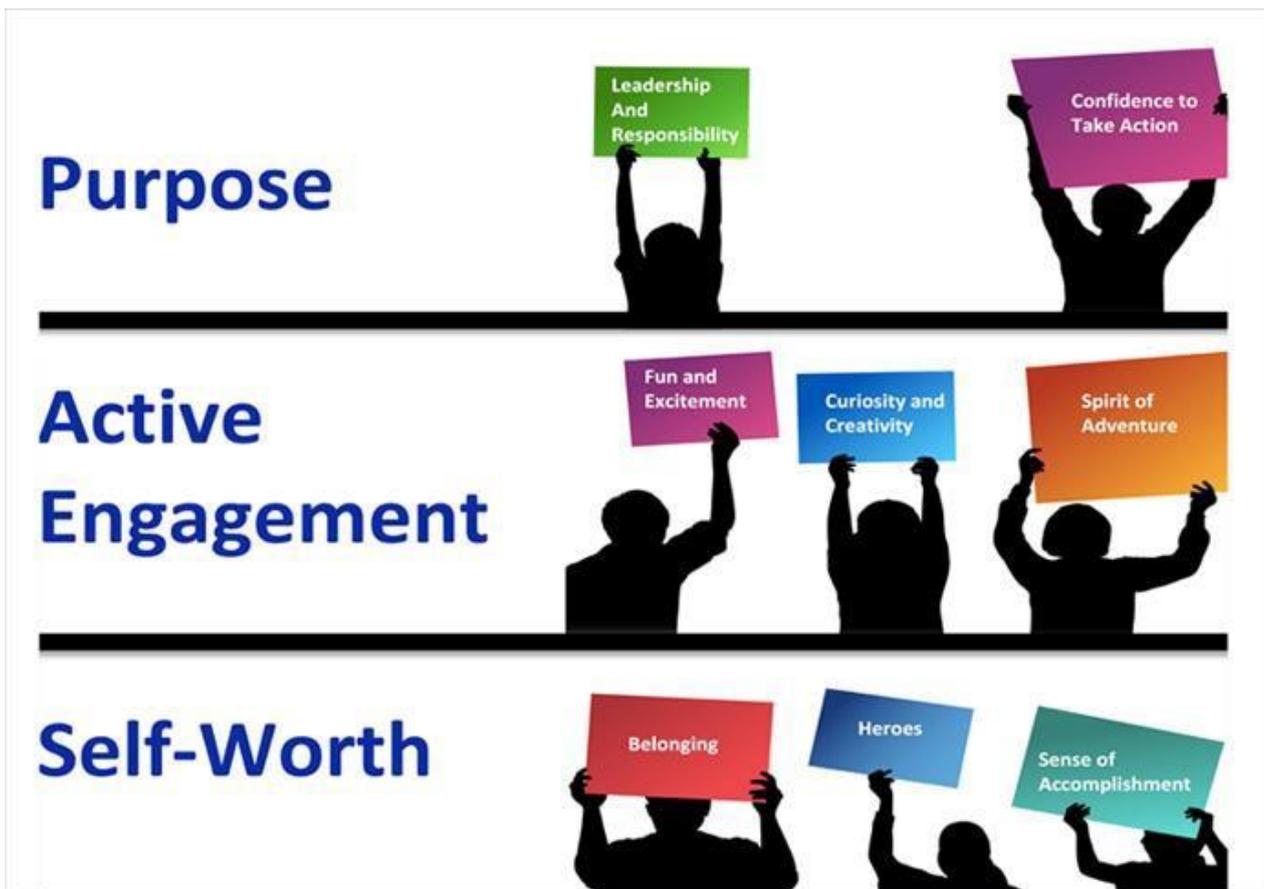




Oak Hill Academy



E-Safety Policy

Draft to SLT: 19th Nov 2019

Approved by staff: 26th Nov 2019

E-SAFETY

E-Safety is a vital part of our curriculum at Oak Hill Academy. We have an up to date policy which demonstrates how we keep our children safe online. Alongside this we our E-Safety Curriculum helps the children learn about how to keep themselves safe when using the internet and digital technologies. Our Internet Safety Rules are displayed around the school, regular theme weeks and assemblies are held to support the promotion of E-Safety. We have devised a Parents' Guide to E-safety booklet available on our school website and in our school reception area. We organise parents' workshops to help parents understand their role in keeping their children safe when using ICT. Our Technology Ambassadors, who are democratically elected from all classes across the school, work strategically to bring about positive changes to our taught e-safety curriculum.

Scope of the Policy

This policy applies to all members of the *academy* (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 *academy*.

The Education and Inspections Act 2006 empowers Principals to such extent as is reasonable, to regulate the behaviour of pupils 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 e-safety 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 (see appendix for policy). 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 e-safety behaviour that take place out of academy.

Roles and Responsibilities

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

Governors:

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the *Governors* receiving regular information about e-safety incidents and monitoring reports. A member of the *Governing Body (Dee Howley)* has taken on the role of *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 / Board / committee / meeting*

Principal and Senior Leaders:

- **The Principal has a duty of care for ensuring the safety (including e-safety) of members of the academy community**
- **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.**
- *The Principal and Senior Leaders are responsible for ensuring that the E-Safety Coordinator 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 Principal will ensure that there is a system in place to allow for monitoring and support of those in the academy 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 (DSP):

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

Network Manager / Technical staff:

The *Co-ordinator for ICT / Computing* 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 e-safety technical requirements and any *AAT* Guidance that may apply.**
- **that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed**
- that they keep up to date with 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 / internet / Virtual Learning Environment / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Principal / Principal / Senior Leader; E-Safety Coordinator

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 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 Principal for investigation / action / sanction**
- **all digital communications with pupils / parents / carers should be on a professional level and only carried out using official academy systems**
- e-safety issues are embedded in all aspects of the curriculum and other activities
- pupils understand and follow the e-safety and acceptable use policies
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations

- they monitor the use of digital technologies, cameras etc in lessons and other academy activities (where allowed) and implement current policies with regard to these devices
- in lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Child Protection / Safeguarding Designated Person

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

Pupils:

- **are responsible for using the academy's digital technology systems in accordance with the Pupil Acceptable Use Policy**
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand 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 academy and realise that the academy's E-Safety Policy covers their actions out of the academy, if related to their membership of the academy

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 and information about national / local e-safety campaigns. Parents and carers will be encouraged to support the academy in promoting good e-safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at academy events
- access to parents' sections of the website
- their children's personal devices in the academy (where this is allowed)

Community Users

Community Users who access academy systems / website as part of the wider academy provision will be expected to sign a Community User AUA before being provided with access to academy systems.

Policy Statements

Education – pupils

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

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 is provided as part of Computing / PHSE / other lessons and is regularly revisited**
- **Key e-safety messages are reinforced as part of a planned programme of assemblies and pastoral activities**
- **Pupils are 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.**
- **Pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet**
- *Pupils are helped to understand the need for the pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside academy*
- *Staff act as good role models in their use of digital technologies, the internet and mobile devices*
- *In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.*
- *Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.*

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

- Curriculum activities
- Letters, newsletters, website,
- Parents / Carers evenings / sessions
- High profile events / campaigns eg Safer Internet Day
- Reference to the relevant web sites / publications

Education – The Wider Community

The academy will provide opportunities for local community groups / members of the community to gain from the academy's e-safety 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
- E-Safety messages targeted towards grandparents and other relatives as well as parents.
- The academy / academy website will provide e-safety information for the wider community

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:

- **A 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 e-safety training as part of their induction programme, ensuring that they fully understand the academy e-safety policy and Acceptable Use Agreements.**
- The E-Safety Coordinator (or other nominated person) will receive regular updates through attendance at external training events (eg from 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.

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 / 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
- Participation in academy training / information sessions for staff

Technical – infrastructure / equipment, filtering and monitoring

The academy will be responsible for ensuring that the academy 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:

- **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 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.**
- **The ICT 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.**
- *Academy technical staff regularly monitor and record the activity of users on the academy technical systems and users are made aware of this in the Acceptable Use Agreement*

- *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 academy systems and data. These are tested regularly. The academy 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 academy systems.
- *Personal data cannot be sent over the internet or taken off the academy site unless safely encrypted or otherwise secured.*

Use of digital and video images

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

- **When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet 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 academy events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone’s privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other pupils in the digital / video images.
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow the academy policies concerning the sharing, distribution and publication of those images. Those images should only be taken on academy equipment, the personal equipment of staff must not be used for such purposes.
- *Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the academy into disrepute.*
- *Pupils must not take, use, share, publish or distribute images of others without their permission*
- *Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.*
- *Pupils’ full names will not be used anywhere on a website or blog, particularly in association with photographs.*
- *Parents or carers give permission for photographs of their child to be published on the academy website*

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate

- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

The 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".**
- **It has a Data Protection 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.**

Communications

When using communication technologies the academy 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 pupils should therefore use only the academy email service to communicate with others when in academy, 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 pupils or parents / carers (email) 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.
- Pupils at KS2 will be provided with individual academy email addresses for educational use.
- 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 academy website and only official email addresses should be used to identify members of staff.

Social Media - Protecting Professional Identity

All academies and local authorities have a duty of care to provide a safe learning environment for pupils 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.

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 academy or brings the academy into disrepute				X	
Using academy systems to run a private business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the academy / 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			

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

Academy staff should ensure that:

- No reference should be made in social media to pupils, parents / carers or academy staff
- They do not engage in online discussion on personal matters relating to members of the academy community
- Personal opinions should not be attributed to the *academy* or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

The *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. All staff are expected to comply with the Social Networking policy.

Unsuitable / inappropriate activities

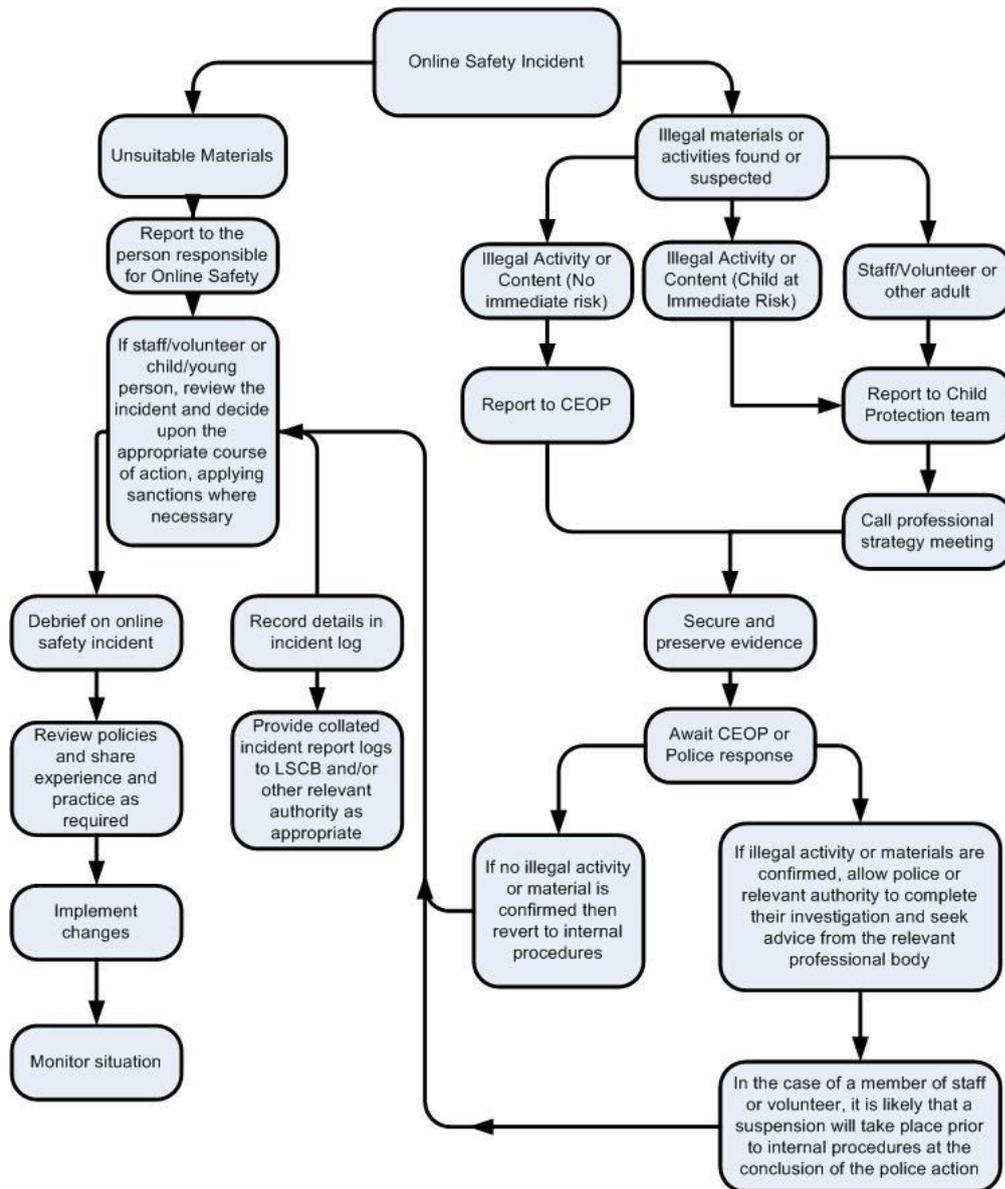
The academy believes that the activities referred to in the following section would be inappropriate in a academy context and that users, as defined below, should not engage in these activities in academy or outside academy when using academy equipment or systems. The academy policy restricts usage as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

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).

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 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.

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 academy 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

Incidents:	Refer to class teacher	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
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X					
Unauthorised use of non-educational sites during lessons	X						X	
Unauthorised use of mobile phone / digital camera / other mobile device	X	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 academy network by sharing username and passwords	X						X	
Attempting to access or accessing the academy network, using another student's / pupil's account	X						X	
Attempting to access or accessing the academy network, using the account of a member of staff		X			X			X
Corrupting or destroying the data of other users				X				X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		X	X		X			X
Continued infringements of the above, following previous warnings or sanctions		X		X				X
Actions which could bring the academy into disrepute or breach the integrity of the ethos of the academy		X		X				X
Using proxy sites or other means to subvert the academy's / academy's filtering system					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
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act		X						X

Staff

Actions / Sanctions

Incidents:	Refer to line manager	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				X
Inappropriate personal use of the internet / social media / personal email	X	X				X		
Unauthorised downloading or uploading of files	X				X	X		
Allowing others to access academy network by sharing username and passwords or attempting to access or accessing the academy 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
Actions which could compromise the staff member's professional standing		X	X					X
Actions which could bring the academy into disrepute or breach the integrity of the ethos of the academy		X					X	
Using proxy sites or other means to subvert the academy's filtering system	X					X	X	
Accidentally accessing offensive or pornographic material and failing to report the incident		X	X					
Deliberately accessing or trying to access offensive or pornographic material				X			X	
Breaching copyright or licensing regulations		X						X
Continued infringements of the above, following previous warnings or sanctions		X					X	X