DUKES AND DUCHESSES OF CAMBRIDGE ACADEMY

Last reviewed: 2020

To be reviewed: 2021

eSafety Policy

Key document details			
Author:	ICT Director	**Approver:**	CEO
Owner:	ICT	**Version no.:**	1.0
Draft Date:	March 2019	**Next review:**	March 2019
Ratified:	March 2019		

Contents

1. Development / Monitoring / Review of this Policy.....3

2. Schedule for Development / Monitoring / Review.....3

3. Scope of the Policy.....3

4. Roles and Responsibilities
- 4.1 Principal and Senior Leaders:..... 4
- 4.2 e-Safety Coordinator / Officer:.....4
- 4.3 IT Technical Support Team:..... 5
- 4.4 Teaching and Support Staff:..... 5
- 4.5 Child Protection / Safeguarding Designated Person / Officer:.....5
- 4.6 Students / Pupils:.....6
- 4.7 Parents / Carers..... 6
- 4.8 Community Users.....6

5. Policy Statements
- 5.1 Education – Students / Pupils.....6
- 5.2 Education – Parents / Carers..... 7
- 5.3 Education & Training – Staff / Volunteers..... 7
- 5.4 Training – Governors..... 8
- 5.5 Technical – Infrastructure / Equipment, Filtering and Monitoring..... 8
- 5.6 Federation and Academy Security Policies..... 9
- 5.7 Personal Devices 9
- 5.8 Use of digital and video images.....10
- 5.9 Data Protection.....11
- 5.10 Communications.....13
- 5.11 Social Media - Protecting Professional Identity.....14

6. Unsuitable / Inappropriate Activities..... 15

7. Responding to incidents of misuse
- 7.1 Illegal Incidents..... 16
- 7.2 Other Incidents..... 16
- 7.3 Academy Actions & Sanctions..... 17

1. Development / Monitoring / Review of this Policy

This e-Safety policy has been developed by a working group / committee made up of:

- Federation Staff
- Principal / Senior Leaders
- E-Safety Officer / Coordinator
- Governors / Board

2. Schedule for Development / Monitoring / Review

This e-Safety policy was approved by the *Board of Directors / Governing Body / Governors Committee on:*	*September 2020*
The implementation of this e-Safety policy will be monitored by the:	
Monitoring will take place at regular intervals:	*Termly*
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:	*Annually*
The E-Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-Safety or incidents that have taken place. The next anticipated review date will be:	*August 2021*
Should serious e-Safety incidents take place, the following external persons / agencies should be informed:	*DADOC Designated Safeguarding Officer* _____ *Head of Academy*

3. 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 Academy.

The Education and Inspections Act 2006 empowers Principals to such extent as is reasonable, to regulate the behaviour of students / 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.

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.

4. Roles and Responsibilities

The following section outlines the e-Safety roles and responsibilities of individuals and groups within the Academy.

4.1 Principal and Senior Leaders:

- The Principal has a duty of care for ensuring the safety (including e-Safety) of members of the Academy community, though the day to day responsibility for e-Safety will be delegated to the E-Safety Co-ordinator / Officer.
- The Principal and (at least) another member of the Senior Leadership Team/ Senior Management Team should be aware of the procedures to be followed in the event of a serious e-Safety allegation being made against a member of staff. (see flow chart on dealing with e-Safety incidents).
- The Principal / Senior Leaders are 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 Principal / Senior Leaders 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.
- The Senior Leadership Team / Senior Management Team will receive regular monitoring reports from the E-Safety Co-ordinator / Officer.

4.2 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 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 Federation/ 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 the E-Safety Governor to discuss current issues, review incident logs and filtering / change control logs.
- attends relevant meeting / committee of Governors.
- reports regularly to the Senior Leadership Team.

4.3 IT Technical Support Team:

The IT technical support team 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 Federation/ 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 that 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 / internet / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Principal / Senior Leader; E-Safety Coordinator / Officer for investigation / action / sanction.
- that monitoring software / systems are implemented and updated as agreed in Academy policies.

4.4 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 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 / Senior Leader ; E-Safety Coordinator / Officer for investigation / action / sanction.
- all digital communications with students / 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.
- students / pupils understand and follow the e-Safety and acceptable use policies.
- students / 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, mobile devices, 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 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.

4.5 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

4.6 Students / Pupils:

- are responsible for using the Academy digital 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 Academy and realise that the E-Safety Policy covers their actions out of Academy, if related to their membership of the Academy

4.7 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 and information about national / local e-Safety campaigns / literature. 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 and on-line student / pupil records
- their children's personal devices in the Academy (where this is allowed)

4.8 Community Users

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

5. Policy Statements

5.1 Education – Students / Pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students in e-Safety is therefore an essential part of the 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 should be provided as part of Computing / PHSE / other 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 Academy
- 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 (e.g. 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.

5.2 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, web site, VLE
- Parents / Carers evenings / sessions
- High profile events / campaigns e.g. Safer Internet Day
- Reference to the relevant web sites / publications e.g. www.saferinternet.org.uk/ http://www.childnet.com/parents-and-carers

5.3 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 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 e-Safety training as part of their induction programme, ensuring that they fully understand the Academy e-Safety policy and Acceptable Use Agreements.

5.4 Training – Governors

Governors should take part in e-Safety training / awareness sessions, with particular importance for those who are members of any 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 Federation/ National Governors Association / or other relevant organisation.
- Participation in Academy training / information sessions for staff or parents.

5.5 Technical – Infrastructure / Equipment, Filtering and Monitoring

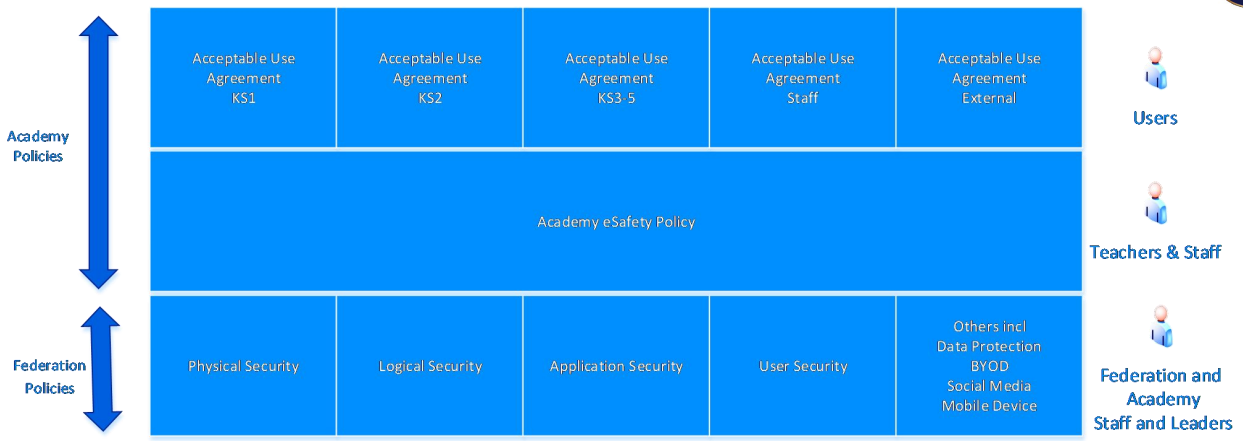
The Academy will be responsible for ensuring that the Academy infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. The Academy will work with the Federation IT team to ensure the network and infrastructure is secure. It will also need to ensure that the relevant roles identified 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, see the relevant Federation IT policies including the User Security Policy, the Physical and Logical security policies. This policy must be read in conjunction with the other relevant Local and Federation Policies, see diagram below.
- 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, see Federation Physical Security Policy.
- All users will have clearly defined access rights to Academy technical systems and devices, see Federation Logical Security Policy and Application Security Policy.
- All users at Key Stage 2 and above will be provided with a username and secure password by the IT team 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. Class logins are acceptable for Key Stage 1 classes.

- All local IT staff will use their "normal" account for day-to-day duties and will only use their delegated Admin username when required. Delegated Admin credentials must never be given out to non IT team members. Users allocated Delegated Admin accounts must be recorded by the central team.
- The IT Team 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. Non IT staff and students should not attempt to install or copy unauthorised software on to Federation devices or install Federation software on to personal devices, unless authorised by the
  IT team.
- Internet access is filtered for all users. Illegal content e.g. child sexual abuse images is filtered by the LGfL and internally 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.
- The Federation IT team 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.
- An appropriate system is in place, via the Service Desk 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 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" (e.g. trainee teachers, supply teachers, visitors) onto the Academy systems, see Federation User Security Policy.
- An agreed policy is in place, see User Security Policy that forbids staff from downloading executable files and installing programs on Academy devices.
- An agreed policy is in place regarding the use of removable media (e.g. memory sticks / CDs / DVDs) by users on Academy devices. Personal data cannot be sent over the internet or taken off the Academy site unless safely encrypted or otherwise secured. (see Federation Data Protection Policy).

5.6 Federation and Academy Security Policies



5.7 Personal Devices

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 of users bringing their own technologies in order to provide a greater freedom of choice and usability. However, there are a number of e-Safety considerations for personal device security that need to be reviewed prior to implementing such a policy. Use of personal devices 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, see Federation Personal Device Security Policy.

- The Academy has a set of clear expectations and responsibilities for all users
- The Academy 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 Academy's normal filtering systems, while being used on the premises
- All users will use their username and password and keep this safe
- Students / Pupils receive 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 Personal Device Security policy

5.8 Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students / pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers

and students / 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 students / pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- 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 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 / pupils in the digital / video images.
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow 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 should not be used for such purposes.
- Care should be taken when taking digital / video images that students / pupils are appropriately dressed and are not participating in activities that might bring the individuals or the Academy into disrepute.
- Students / pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include students / pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Students' / Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of students / pupils are published on the Academy website.
- Student's / Pupil's work can only be published with the permission of the student / pupil and parents or carers.

5.9 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.
- It complies with the Federation Data Protection Policy.
- It is registered as a Data Controller for the purposes of the Data Protection Act (DPA) or comes under the Federation Data Protection Umbrella.
- 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.

- Comply with the Federation User Security Policy.

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 with a strong password.
- the device must 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 Academy policy once it has been transferred or its use is complete.

5.10 Communications

Communication Technologies	Staff & other adults				Students / Pupils			
	Allowed	Allowed nes	Allowed staff	Not	Allowed	Allowed nes		Not
Mobile phones may be brought to Academy	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 e.g. tablets, gaming devices				X				X
Use of personal email addresses in Academy, or on Academy network				X				X
Use of Academy email for personal emails				X				X
Use of messaging apps	X							X
Use of social media	X							X
Use of blogs	X							X

*Move and insert X where appropriate

A wide range of rapidly developing communications technologies has the potential to enhance learning. 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 students / pupils should therefore use only the Academy email service

to communicate with others when in Academy, or on Academy systems (e.g. 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 / pupils 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.
- Whole class / group email addresses may be used at KS1, while students / pupils at KS2 and above will be provided with individual Academy email addresses for educational use.
- 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 Academy website and only official email addresses should be used to identify members of staff.
- Staff should never use personal email or other personal social media accounts to communicate with students.
- Where staff use externally hosted web sites and services these must be registered with the Principal and IT team. Any Admin level user names and passwords should also be registered with the local IT team.
- All communications need to be in accordance with the Federation "Code of Conduct" available on HarrisNet policies area.

5.11 Social Media - Protecting Professional Identity

All Academies and Federations have a duty of care to provide a safe learning environment for pupils and staff. Academies and Federations 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 Federation liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

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 students / 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.
- No communication with students using personal accounts.

The Academy's use of social media for professional purposes will be checked regularly by the Senior Safeguarding Officer to ensure compliance with the Social Media, Data Protection Policies.

6. 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	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	**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	

contain or relate to:	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					X	
Infringing copyright						X
Revealing or publicising confidential or proprietary information (e.g. 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 e.g. YouTube				X		

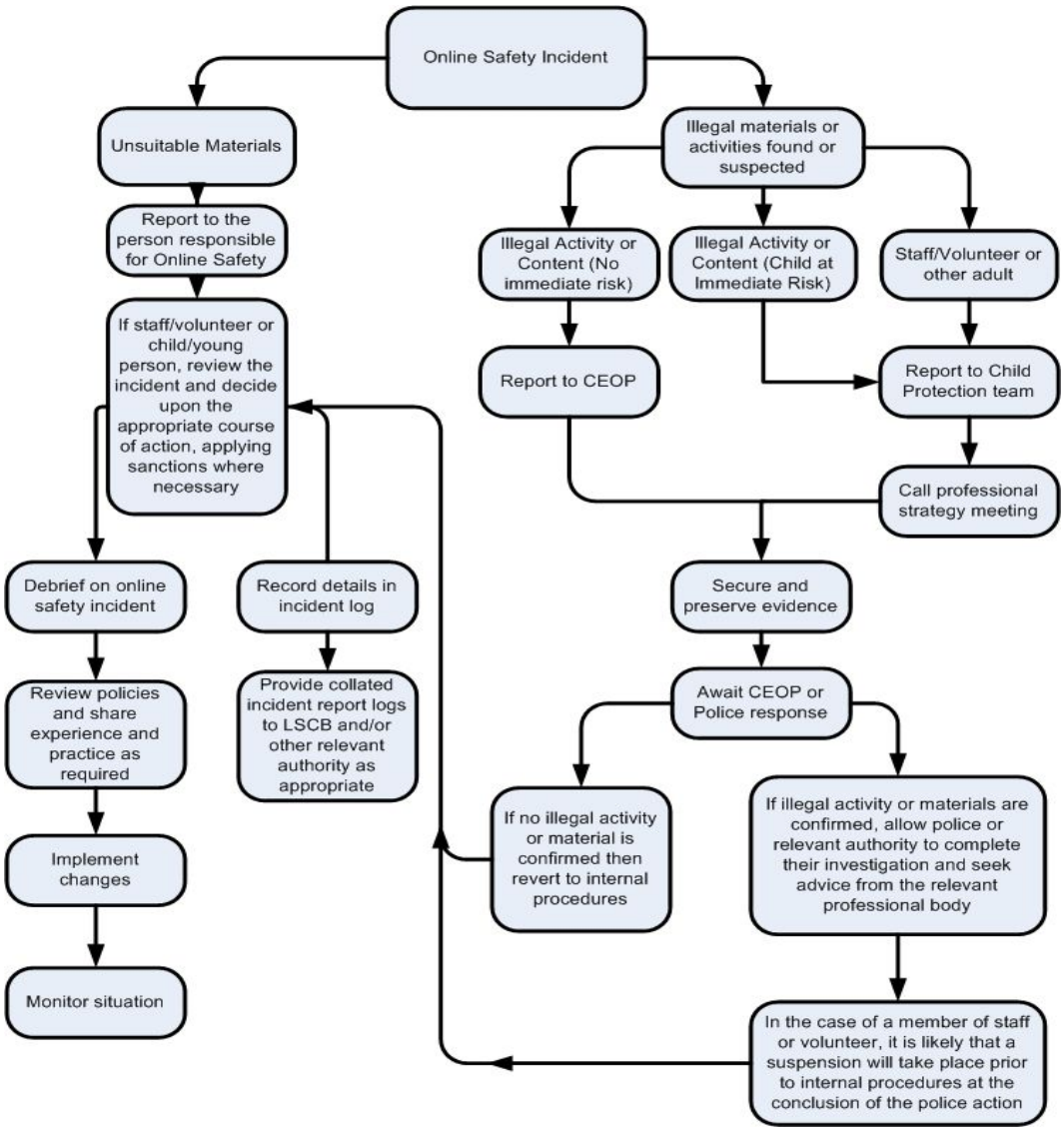
* Move and insert x where appropriate

7. 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).

7.1 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.



7.2 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.
- The Principal must be notified of and approve the investigation.
- 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 Federation 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.

7.3 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 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	**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	X			
Unauthorised use of non-educational sites during lessons	X		X		X	X			
Unauthorised use of mobile phone / digital camera / other mobile device	X		X			X			X
Unauthorised use of social media / messaging apps / personal email	X		X			X			X
Unauthorised downloading or uploading of files	X		X		X	X			X
Allowing others to access Academy network by sharing username and passwords	X		X			X			X
Attempting to access or accessing the Academy network, using another student's / pupil's account	X		X			X			X
Attempting to access or accessing the Academy network, using the account of a member of staff	X		X			X			X
Corrupting or destroying the data of other users	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
Continued infringements of the above, following previous warnings or sanctions	X		X	X		X			X
Actions which could bring the Academy into disrepute or breach the integrity of the ethos of the Academy	X		X			X			X
Using proxy sites or other means to subvert the 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			X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	X		X	X		X			X

*Move and insert x where appropriate

Staff	Actions / Sanctions							
Incidents:	Refer to line manager	Refer to Principal	Refer to Federation/ 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	X
Inappropriate personal use of the internet / social media / personal email		X				X		
Unauthorised downloading or uploading of files		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		
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
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	X			X	X	X
Actions which could bring the Academy into disrepute or breach the integrity of the ethos of the Academy		X	X			X	X	X
Using proxy sites or other means to subvert the Academy's filtering system		X	X			X	X	X
Accidentally accessing offensive or pornographic material and failing to report the incident		X	X			X		
Deliberately accessing or trying to access offensive or pornographic material		X	X	X			X	X

Storing or transferring confidential personal data on unencrypted devices		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	

*Move and insert x where appropriate