# E-safety Policy

## Document Control

| | |
|---|---|
| **Version Number:** | 2 |
| **Applicable To:** | Trust & All Academies |
| **Committee:** | Values all Students<br>IT Directorate |
| **Approved By Executive Board in:** | September 2019 |
| **Review Cycle:** | Every two years |
| **Date of Next Review:** | September 2021 |
| **Related Policies:** | CMAT Data Protection & Freedom of Information Policy (GDPR)<br>CMAT Staff code of conduct<br>CMAT Disciplinary Procedures (Staff)<br>CMAT IT & Acceptable Use Policy<br>CMAT Child Protection and Safeguarding policy<br>CMAT Search & Confiscation Policy<br>Academy Behaviour Policy<br>Academy policy on the use of mobile technology including phones |

## Revisions

| Version | Page/Para No. | Description of Change | Approved |
|---|---|---|---|
| 2 | | Links to related Policies<br>Correction of terminology following GDPR<br>Format up date | September 2019 |
| | | | |

**Contents page**

## 1 Introduction

The key issues around E-safety affect all Academies across the Trust and as such this policy was produced following consultation throughout the Trust.

Should serious E-safety incidents take place within any CMAT Academy, the CEO and Director of IT will be notified.

Each Academy will monitor the impact of the policy using a range of appropriate methods. This may include:

- Logs of reported incidents
- Annual reports to the Academy Council
- Monitoring logs of internet activity (including sites visited)
- Internal monitoring data for network activity
- Surveys / questionnaires of
- students / pupils
- parents / carers
- staff

The implementation of this E-safety policy will be monitored by the:

- IT Area Manager,
- E Safety Co-Ordinator
- Principal

The Academy Council will receive a report on the implementation of the E-safety Policy at regular intervals.

The E-safety Policy will be reviewed every two years 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.

Should serious E-safety incidents take place, the Trust/Academy will refer to the Child Protection and Safeguarding Policy, as appropriate.

## 2 Scope of the Policy

This policy applies to all members of the CMAT 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 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 each 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 which is unique to each Academy.

Each Academy across the Trust 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.

## 3 Roles and Responsibilities

The following section outlines the E-safety roles and responsibilities of individuals and groups within the Academy:

**Academy Councillors (AC)**
AC members are responsible for the application of the E-safety Policy at a local level and for reviewing the effectiveness of the policy for each Academy. This will be carried out by the AC members receiving regular information about E-safety incidents and monitoring reports. At each Academy, E-safety issues will fall under the remit of the Academy Council. A member of the Academy Council should be given the role of E-safety councillor; this is often linked to the role of the Safeguarding Champion. The role of the E-safety councillor will include:

- meetings with the E-safety Co-ordinator for their Academy
- monitoring of E-safety incident logs
- reporting at the Academy Council meetings

**Principal and Senior Leaders**
The Principal has a duty of care for ensuring the safety (including E-safety) of all members of the Academy community, though the day to day responsibility for E-safety will be delegated to the E-safety Co-ordinator.

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 E-safety incidents – included in a later section – "Responding to incidents of misuse" in section 10 and relevant CMAT staff disciplinary procedures and related policies).

The Principal / 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 / 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 will receive regular monitoring reports from the E-safety Co-ordinator.

**The E-safety Coordinator:**
The E-safety coordinator:

- takes day to day responsibility for E-safety issues and has a leading role in establishing and reviewing the Academy E-safety procedures
- ensures that all staff are aware of the procedures that need to be followed in the event of an E-safety incident taking place
- keeps up to date with E-safety information in order to effectively carry out their E-safety role and to inform and update others as relevant
- provides training and advice for staff
- liaises with the Local Authority / relevant body
- liaises with Academy/ Trust technical staff
- receives reports of E-safety incidents and creates a log of incidents to inform future E-safety developments
- meets every year with E-safety Academy Champion; often the Safeguarding Champion; and IT technical staff to discuss current issues, review incident logs and filtering / change control logs
- attends relevant meetings

- reports annually to Senior Leadership Team

In many cases issues relating to E-safety will also have a related safeguarding aspect. With this in mind it is vital that the E-safety Co-ordinator also has relevant and up-to-date safeguarding training.

**IT Area Manager**
The IT Manager 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 Local Authority 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
- 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 E-safety Co-ordinator for investigation / action / sanction / logging
- that reports from web filtering and DNA monitoring is sent to the senior tutor promptly

**Teaching and Support Staff**
Staff are responsible for ensuring that:

- they have an up to date awareness of E-safety matters and of the current Trust E-safety policy and practices
- they have read, understood and signed the IT Acceptable Use Policy (AUP)
- they report any suspected misuse or problem to the Senior Leader / E-safety Coordinator 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 aspects of the curriculum and other activities
- students understand and follow the E-safety and acceptable use policies
- students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other Academy activities (where allowed) and implement current policies with regard to these devices
- in lessons where internet use is pre-planned 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

**Child Protection / Designated Safeguarding 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
- sexting

**Students / pupils:**

- are responsible for using the Academy digital technology systems in accordance with the Acceptable Use Policy (AUP)

- 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 hours and realise that the Academy's E-safety Policy covers their actions out of Academy hours, 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 / VLE and information about national or local E-safety campaigns and relevant 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 / VLE and on-line student / pupil records
- their children's personal devices

## 4 Education and developing understanding

**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 their Academy to recognise and avoid E-safety risks and build their resilience.

E-safety should be 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 / reviewed
- 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 subjects 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
- 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.

**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.

Academies across the Trust will therefore seek to provide information and awareness to parents and carers through:

- An E-safety guidance page on each Academy/academy website
- Curriculum activities
- Letters, newsletters, website
- Parents / Carers evenings / sessions
- Reference to relevant web sites / publications e.g.
    - www.swgfl.org.uk
    - www.saferinternet.org.uk
    - www.childnet.com/parents-and-carers
    - www.ceop.org
- Identification of the named E-safety co-ordinator in each Academy should be available on each Academy website

**Education & Training – Staff / Volunteers**
It is essential that all staff receive E-safety training and understand their responsibilities, as outlined in this policy. E-safety issues often relate to issues around safeguarding and staff should ensure they consider this aspect when responding to issues. 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 periodically.
- 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.
- This E-safety Policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.
- The E-safety Coordinator (or other nominated person) will provide advice, guidance and training to individuals as required.

**Technical – infrastructure / equipment, filtering and monitoring**
The Trust 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 discussed 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.
- Global "admin" passwords for the Academy must not be shared. Accounts with "admin rights" must be reviewed regularly and restricted to those who require them. Eligibility and permission rights are controlled and monitored by the Trust's Director of IT and Technical Services Manager.

- The IT area 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 Trust or internet provider by actively employing the Internet Watch Foundation Policy 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.
- 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.
- 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, workstations, 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.
- An agreed policy is in place regarding the extent of personal use that users (staff / students / pupils / community users) and their family members are allowed on Academy devices that may be used out of Academy.

**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 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 students 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, if personal equipment is the only device available then staff may use this, copy the material to the Academy network and then remove the material from their device within a reasonable amount of time or ideally as soon as possible.
- 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 work can only be published with the permission of the student / pupil and parents or carers.

## 5 Data Protection

Personal data will be recorded, processed, transferred and made available according to the current CMAT Data Protection & Freedom of Information Policy (GDPR) which ach Academy and all its members must adhere to.

## 6 Communication

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.
- Users must immediately report, to the nominated person 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.
- 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 will not use personal e-mail account to communicate with anyone in the Academy community (I.e: Students, Staff, Parents, AC/Governors, Local Authority, Local parish/district councils).

## 7 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.

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.

The use of social media for professional purposes will be checked regularly by the Principal and E-safety committee to ensure compliance with all related policies

## 8 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 the normal behaviour / disciplinary policy.

Sanctions include any laid out in the Academy Behaviour Policy and CMAT Human Resources (HR) Policies.

Examples of things that could cause sanctioned are below:

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

## 9 Unsuitable / inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from the Academy and all other technical systems. Other activities e.g. cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in an educational context, either because of the age of the users or the nature of those activities. The table on the following page offers further guidance on these activities.

The Trust believes that the activities referred to in the following section would be inappropriate in an Academy context and those users, as defined below, should not engage in these activities in an Academy or outside the Academy when using Academy equipment or systems. This Policy restricts usage as follows:

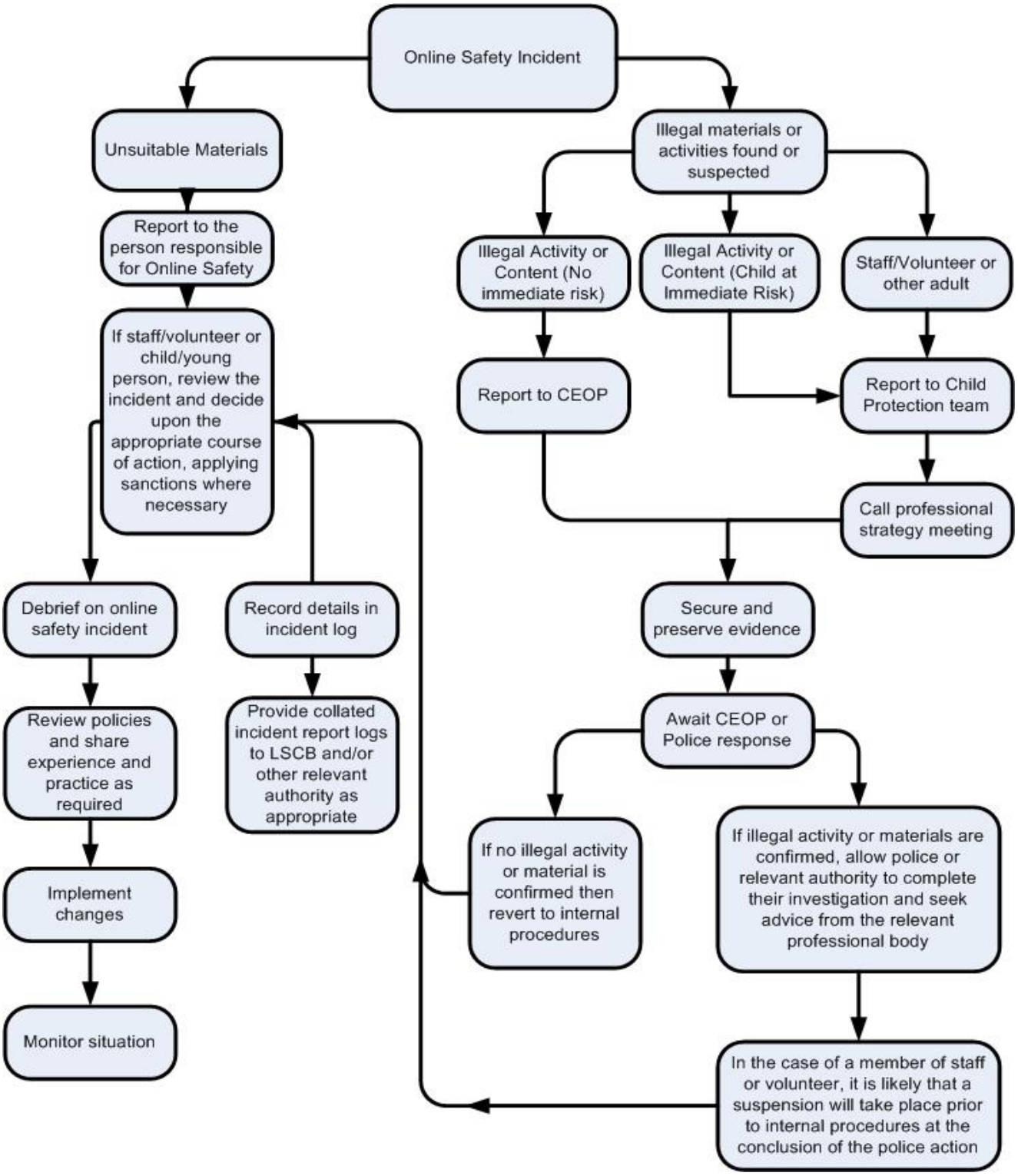
| **User Actions** | | Acceptable | Acceptable at certain times | Acceptable for nominated users | Unacceptable | Unacceptable and illegal |
|---|---|---|---|---|---|---|
| Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals 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 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 (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 | |

## 10 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

### Illegal Incidents

If there is any suspicion that the website(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 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 and refer to the CMAT Child Protection and Safeguarding Policy)
- 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 and recent iterations of this 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.

**Sexting**
Sexting is defined as 'Images or videos generated of/by children under the age of 18 that are of a sexual nature or are indecent. These images are shared between young people and/or adults via a mobile phone, handheld device or website with people they may not even know.'

Sexting is an increasing issue and as such specific advice and guidance has been published entitled '*Sexting in Schools: advice and support around self-generated images'*. All CMAT Academies will ensure they adopt and follow this guidance, and that all issues of sexting are reported to and discussed with the Child Protection and Safeguarding Lead within the Academy.

**APPENDIX A**: **Legislation**

Academies should be aware of the legislative framework under which this E-safety Policy template and guidance has been produced. It is important to note that in general terms an action that is illegal if committed offline is also illegal if committed online.

It is recommended that legal advice is sought in the event of an E-safety issue or situation. The list below is not an exhaustive list, however the most recent iteration of these acts should be applied.

**Computer Misuse Act 1990**
This Act makes it an offence to:

- Erase or amend data or programs without authority;
- Obtain unauthorised access to a computer;
- "Eavesdrop" on a computer;
- Make unauthorised use of computer time or facilities;
- Maliciously corrupt or erase data or programs;
- Deny access to authorised users.

**General Data Protection Act 2018**
This protects the rights and privacy of individual's data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Act states that person data must be:

- Fairly and lawfully processed.
- Processed for limited purposes.
- Adequate, relevant and not excessive.
- Accurate.
- Not kept longer than necessary.
- Processed in accordance with the data subject's rights.
- Secure.
- Not transferred to other countries without adequate protection.

**Freedom of Information Act 2000**
The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures.

**Communications Act 2003**
Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

**Malicious Communications Act 1988**
It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.

**Regulation of Investigatory Powers Act 2000**
It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to:

- Establish the facts;
- Ascertain compliance with regulatory or self-regulatory practices or procedures;

- Demonstrate standards, which are or ought to be achieved by persons using the system;
- Investigate or detect unauthorised use of the communications system;
- Prevent or detect crime or in the interests of national security;
- Ensure the effective operation of the system.
- Monitoring but not recording is also permissible in order to:
- Ascertain whether the communication is business or personal;
- Protect or support help line staff.
- The Academy reserves the right to monitor its systems and communications in line with its rights under this act.

**Telecommunications Act 1984**
It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

**Criminal Justice & Public Order Act 1994**
This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they:

- Use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or
- Display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

**Racial and Religious Hatred Act 2006**
This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

**Protection of Children Act 1999**
It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is a anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison

**Sexual Offences Act 2003**
The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

**Obscene Publications Act 1959 and 1964**
Publishing an “obscene” article is a criminal offence. Publishing includes electronic transmission.

**The Education and Inspections Act 2006**
Empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the Academy site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.

**The Education and Inspections Act 2011**

Extended the powers included in the 2006 Act and gave permission for Headteachers (and nominated staff) to search for electronic devices. It also provides powers to search for data on those devices and to delete data.

**The Protection of Freedoms Act 2012**
Requires Academies to seek permission from a parent / carer to use Biometric systems

**The Academy Information Regulations 2012**
Requires Academies to publish certain information on its website

## APPENDIX B: Links to other organisations or documents

The following links may be useful when reviewing or applying the Academy E-safety policy.

https://www.saferinternet.org.uk/

https://www.childnet.com

https://www.saferinternet.org.uk/our-helplines

https://www.iwf.org.uk

https://www.ceop.police.uk/safety-centre/

https://www.thinkuknow.co.uk