David Ross Education Trust

Broadening Horizons

DRET E-Safety Policy

Introduction/Overview

The safety of our community online is our highest priority in using information and communications technology in our Trust. The contents of this policy and data protection policy take precedence over any other procedures or systems.

This policy uses the term students to refer to the children and young people at the institution.

Unless recorded elsewhere at the Academy the default position set out in this policy applies.

Policy			
Version	Date Approved by Trustees	Date Released to Academies	Next Review Date
V1.0	28 June 2016	1 September 2016	January 2018

1. Background

1.1 New technologies have become integral to the lives of children and young people in today's society, both our academy and in their lives outside school.

1.2 The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and students learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe internet access at all times.

1.3 The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in our academy are bound. Our E-Safety policy helps to ensure safe and appropriate use. The development and implementation of such a strategy involves all the stakeholders in a child's education from the Trust, Principal and governors to the senior leaders and classroom teachers, support staff, parents, members of the community and the students themselves.

1.4 The use of these exciting and innovative tools in academy and at home has been shown to raise educational standards and promote pupil / student achievement.

1.5 However, the use of these new technologies can put young people at risk within and outside the academy. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use, which may impact on the social and emotional development and learning of the young person.

1.6 Many of these risks reflect situations in the off-line world and it is essential that this E-Safety policy is used in conjunction with other academy policies (eg behaviour, anti-bullying and child protection policies).

1.7 As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build student's resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with them.

1.8 E-Safety is not solely an issue for students. The 2012 Teacher Standards document sets out clear expectations for the personal professional conduct of teachers over and above the legal framework covering all adults.

Standard	Relation to policy
PART TWO: PERSONAL AND PROFESSIONAL CONDUCT A teacher is expected to demonstrate consistently high standards of personal and professional conduct. The following statements define the behaviour and attitudes which set the required standard for conduct throughout a teacher's career.	See: ● Roles & responsibilities, teachers & support staff ● Education & training: staff ● Staff and volunteer acceptable use policy In addition
● Teachers uphold public trust in the profession and maintain high standards of ethics and behaviour, within and outside school, by:	… including in electronic communication of all kinds
o treating pupils with dignity, building relationships rooted in mutual respect, and at all times observing proper boundaries appropriate to a teacher's professional position	
o having regard for the need to safeguard pupils' well-being, in accordance with statutory provisions	… applying safeguarding policy and procedure rigorously in the context of E-Safety … including in electronic communication of all kinds
o showing tolerance of and respect for the rights of others o not undermining fundamental British values, including democracy, the rule of law, individual liberty and mutual respect, and tolerance of those with different faiths and beliefs o ensuring that personal beliefs are not expressed in ways which exploit pupils' vulnerability or might lead them to break the law.	
• Teachers must have proper and professional regard for the ethos, policies and practices of the school in which they teach, and maintain high standards in their own attendance and punctuality.	
• Teachers must have an understanding of, and always act within, the statutory frameworks which set out their professional duties and responsibilities.	

1.9 Each academy must demonstrate that it has provided the necessary safeguards to help ensure that they have done everything that could reasonably be expected of them to manage and reduce these risks. The E-Safety policy that follows explains how we intend to do this, while also addressing wider educational issues in order to help young people (and their parents / carers) to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

2. Development/Monitoring/Review of this Policy

2.1 This E-Safety policy has been developed by the Trust IT Team.

2.2 Schedule for Development / Monitoring / Review
This policy will come into effect from September 2016.
It will be reviewed by a panel consisting of the Head of IT & Data, two Principals, one member of technical support staff and one governor in April of each year.
The academy will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited)
- Annual surveys / questionnaires of
- students (eg “Tell-us” survey / CEOP ThinkUknow survey)
- parents / carers
- staff

The results of these surveys will be reviewed each year in June to July and otherwise as required.

3. Scope of the Policy

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

3.2 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 out of academy, but is linked to membership of the academy.

3.3 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

4.1 The following section outlines the roles and responsibilities for E-Safety of individuals and groups within our academy:

4.2 Governors:
Governors are responsible for the being aware of the E-Safety Policy and any optional elements to be adopted at their Academy and for reviewing the effectiveness of the policy. This will be carried out by the Finance and General Purposes Sub-Committee receiving regular information about E-Safety incidents and monitoring reports.

A member of the Governing Body may be designated as the E-Safety Governor which will include:

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

4.3 Principal and Senior Leaders:

- The Principal is responsible for ensuring the safety (including E-Safety) of members of the academy community and direct a member of staff to act as E-Safety Officer.
- *The day to day responsibility for e-safety may be retained by the Principal if required.*
- The Principal / Senior Leaders are responsible for ensuring that they, or the E-Safety Coordinator / Officer and other relevant staff receive suitable CPD 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 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 termly monitoring reports from the E-Safety Co-ordinator / Officer.
- **The Principal and another member of the Senior Leadership Team /Senior Management Team must be aware of the procedures to be followed in the event of a serious E-Safety allegation being made against a member of staff.**

5. E-Safety Coordinator/Officer

- Takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the academy e-safety 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 and Trust staff
- Liaises with academy IT service staff or external contractors
- 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 meeting / committee of Governors
- Reports at least termly to Senior Leadership Team.

6. IT Service Staff

6.1 If an Academy has a managed IT service provided by an outside contractor, it is their responsibility to ensure that the managed service provider carries out all the E-Safety measures that would otherwise be the responsibility of own technical staff, as set out below. It is also important that the managed service provider is fully aware of Data Protection Policy, Security Policy and Acceptable Usage Policy).

6.2 The senior IT service staff member for the Academy is responsible for ensuring:

- that the academy's IT infrastructure is secure and is not open to misuse or malicious attack
- that users may only access the academy's networks through a properly enforced password protection policy, in which passwords are regularly changed
- the broadband service provider is informed of issues relating to the filtering of internet content
- the academy's filtering policy is applied and updated on a regular basis (see section on filtering)
- that he / she keeps 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 use of systems is regularly monitored and logs kept so that misuse can be reported, investigated and sanctioned.
- that monitoring systems are kept up to date and fit for purpose.

7. Teaching and Support Staff

7.1 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 academy Staff Acceptable Use Policy / Agreement (AUP)
- they report any suspected misuse or problem to the E-Safety Co-ordinator / Officer /
- digital communications with students 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 academy activities
- students understand and follow the academy E-Safety and acceptable use policy
- students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor ICT activity in lessons, extra curricular and extended academy activities
- they are aware of E-Safety issues related to the use of mobile devices and that they monitor their use and implement academy policies 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.

8. Designated person for Child Protection/Child Protection Officer

8.1 Should be trained in E-Safety issues and be aware of the potential for serious child protection 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

Some academies may choose to combine the role of Child Protection Officer and E-Safety Officer.

9. Students:

- Are responsible for using the academy IT systems in accordance with the Student / Pupil Acceptable Use Policy, which they will be expected to sign before being given access to academy systems. (NB. at KS1 it would be expected that parents / carers would sign on behalf of the pupils)
- 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 academy policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand academy 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 academy, if related to their membership of the academy

10. Parents/Carers

10.1 Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. In some cases parents and carers will not fully understand the issues and be less experienced in the use of ICT than their children.

10.2 The academy will therefore take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website / VLE and information about national / local E-Safety campaigns / literature.

10.3 Parents and carers will be responsible for:

- Endorsing (by signature) the Student / Pupil Acceptable Use Policy
- Accessing the academy website / VLE / on-line student / pupil records in accordance with the relevant academy Acceptable Use Policy.

11. Community Users

Community Users who access academy IT systems / website / VLE as part of the Extended Academy provision will be expected to sign a Community User AUP before being provided with access to academy systems.

12. Policy Statements

12.1 Education – students

Whilst regulation and technical solutions are very important, their use must be balanced by educating *students* to take a responsible approach. The education of students 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.

12.2 E-Safety education will be provided in the following ways:

- A planned E-Safety programme will be provided as part of the curriculum and should be regularly revisited – this will cover both the use of ICT and new technologies in academy and outside academy
- Key E-Safety messages will be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities
- Students will 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 should be helped to understand the need for the student / pupil AUP and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside academy
- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Rules for use of IT systems / internet will be posted in all rooms and displayed on log-on screens
- Staff should act as good role models in their use of ICT, the internet and mobile devices

12.3 Education – parents/carers

Many parents and carers may 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 experiences. Parents may either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it.

12.4 The academy will therefore not make the assumption that parents and carers are fully aware of the risks of online use and actively seek to provide information and awareness to parents and carers through letters, newsletters, the website, social media and parents evenings.

12.5 Education & Training – Staff

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.
- An audit of the E-Safety training needs of all staff will be carried out annually.
- 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 Policies
- The E-Safety Coordinator (or Principal) will receive regular updates through attendance at training sessions and by reviewing guidance documents released by appropriate bodies.
- 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 / training as required to individuals as required.

12.6 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 ICT / E-Safety / health and safety / child protection. This may be offered in a number of ways:

- Attendance at training provided by the Trust or other relevant organisation.
- Participation in academy training / information sessions for staff or parents

12.7 Technical – infrastructure / equipment, filtering and monitoring

The Regional IT Service Manager will make themselves aware of the provision at each Academy and provide technical guidance as to the effectiveness of the filtering and monitoring systems in place.

12.8 The Trust IT Service 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.

12.9 If the academy has a managed ICT service provided by an outside contractor, it is the responsibility of the academy to ensure that the managed service provider carries out all the E-Safety measures that would otherwise be the responsibility of the academy, as set out here. It is also important that the managed service provider is fully aware of the Security Policy and Acceptable Usage Policy.

12.10 The Academy 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 IT systems will be managed in ways that ensure that the academy meets the e-safety technical requirements outlined in the Acceptable Usage Policy and any relevant Policy and guidance
- There will be regular reviews and audits of the safety and security of academy IT systems as part of the day to day operation of the IT Service
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to academy IT systems. Details of the access rights available to groups of users will be recorded by the Network Manager (or other person) and will be reviewed, at least annually, by the E-Safety Working Group.
- The Trust processes for setting and managing passwords as set out in the IT Handbook will be adhered to.
- Users are responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security to their line manager.
- The Academy maintains and supports the managed filtering service provided by their broadband provider
- A general “base level” of filtering (often called guest access) will ensure that no harmful content is made available to any user over the Academy network.
- A less restrictive “staff level” of filtering, based upon the login profile of each user may be put in place if required.
- If anyone is to be given unfiltered access at any time, this must be recorded in writing and agreed by the E-Safety Officer or Principal. The purpose and duration of the arrangement must be made clear. At the end of the planned period filtering must be restored to previous levels.
- Any filtering issues should be reported immediately to the broadband provider by either the IT Service staff working at the site, the contracted technical staff of the E-Safety Officer.
- Requests from staff for sites to be removed from the filtered list (‘whitelisting’) will be considered by the IT Services staff and E-Safety Officer to ensure protection for the Network Manager or any other member of staff, should any issues arise re unfiltered access. If the request is agreed, this action will be recorded and logged. Such requests will never be handled with less than 24 hours notice and will always be subject to the agreement of two people who are named in the record kept.
- Academy IT Service staff regularly monitor and record the activity of users on the Academy IT systems and users are made aware of this in the Acceptable Use Policy.
- Remote management tools are used by staff to control workstations and view users activity
- Each Academy will put in place an age-approriate system for users to report any actual / potential E-Safety incident to the responsible staff.
- 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.
- An agreed system is in place for the provision of temporary access of “guests” (eg trainee teachers, visitors) onto the Academy system.
- Action is taken to prevent use of unauthorised software by users.

- The academy infrastructure and individual workstations are protected by up to date virus software.
- Users are made aware of data protection policy, good practice and acceptable use policy.

13. Curriculum

13.1 E-Safety should be a focus in all areas of the curriculum and staff should reinforce E-Safety messages in the use of IT across the curriculum.

- In lessons where internet use is pre-planned, it is best practice that students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where students are allowed to freely search the internet, eg using search engines, staff should be vigilant in monitoring the content of the websites the young people visit, and not rely solely on automated protection.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs, discrimination) that would potentially result in internet searches being blocked. In such a situation, staff can request that the Network Manager (and other relevant person) can temporarily whitelist 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.
- Students 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 should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

14. Use of digital and video images – Photographic, Video

14.1 The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff and students need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. The Academy will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm: (select / delete as appropriate)

- When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet eg on social networking sites.
- Staff 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 are appropriately dressed and are not participating in activities that might bring the individuals or the academy into disrepute.
- Students must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images.
- Students' / Pupils' full names will not be used anywhere on a website or blog, when in association with photographs.

- Written permission from parents or carers will be obtained before photographs of students are published by the Academy website.

14.2 Data Protection

See Data Protection policy.

15. Communications

15.1 A wide range of rapidly developing communications technologies has the potential to enhance learning. Each Academy will maintain a copy of the eSafety Communications Permissions Table with it's stated position on usage, within the boundaries set out as acceptable by the Trust in line with decisions made by the Principal.

15.2 Table following table shows how the academy currently considers the benefit of using these technologies for education outweighs their risks / disadvantages:
When deciding their position and 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. Staff and students should therefore use only the academy email service to communicate with others when in academy, or on academy systems (eg by remote access).
- Users need to be aware that email communications may be monitored
- Users must immediately report, to the nominated person – in accordance with the academy policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff and students or parents / carers (email, chat, VLE etc) must be professional in tone and content. These communications may only take place on official (monitored) academy systems. Personal email addresses, text messaging or public chat / social networking programmes must not be used for these communications.
- Whole class or group email addresses will be used at KS1, while students at KS2 and above will be provided with individual academy email addresses for educational use. (Academies may choose to use group or class email addresses for younger age groups eg. at KS1)
- Students should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.
- Personal information should not be posted on the academy website and only official email addresses should be used to identify members of staff.

15.3 Unsuitable / inappropriate activities

Some internet activity eg accessing child abuse images or distributing racist material is illegal and would obviously be banned from academy and all other IT systems. Other activities eg 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 academy context, either because of the age of the users or the nature of those activities.

15.4 The academy believes that the activities referred to in the following section would be inappropriate in an 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 certain internet usage as follows:

15.5 Banned at all DRET Sites

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
- promotion or conduct of illegal acts, eg under the child protection, obscenity, computer misuse and fraud legislation
- incitement to criminal activity
- adult material that potentially breaches the Obscene Publications Act in the UK
- material unsuitable for the age range of students in that institution
- racist material
- pornography
- promotion of any kind of discrimination
- threatening behaviour, including promotion of physical violence or mental harm
- 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
- Gambling

15.6 In addition users will not:

- Use academy systems to run a private business
- Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by academy
- Upload, download or transmit commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions
- Reveal or publicise confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)
- Create or propagate computer viruses or other harmful files
- Carry out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet

15.7 The use of the following categories of service will be determined for each site at the discretion of the Principal as being permitted or banned for staff or for students.

- On-line gaming (educational)
- On-line gaming (non educational)
- On-line shopping / commerce
- File sharing
- Use of social networking sites
- Use of video broadcasting eg Youtube

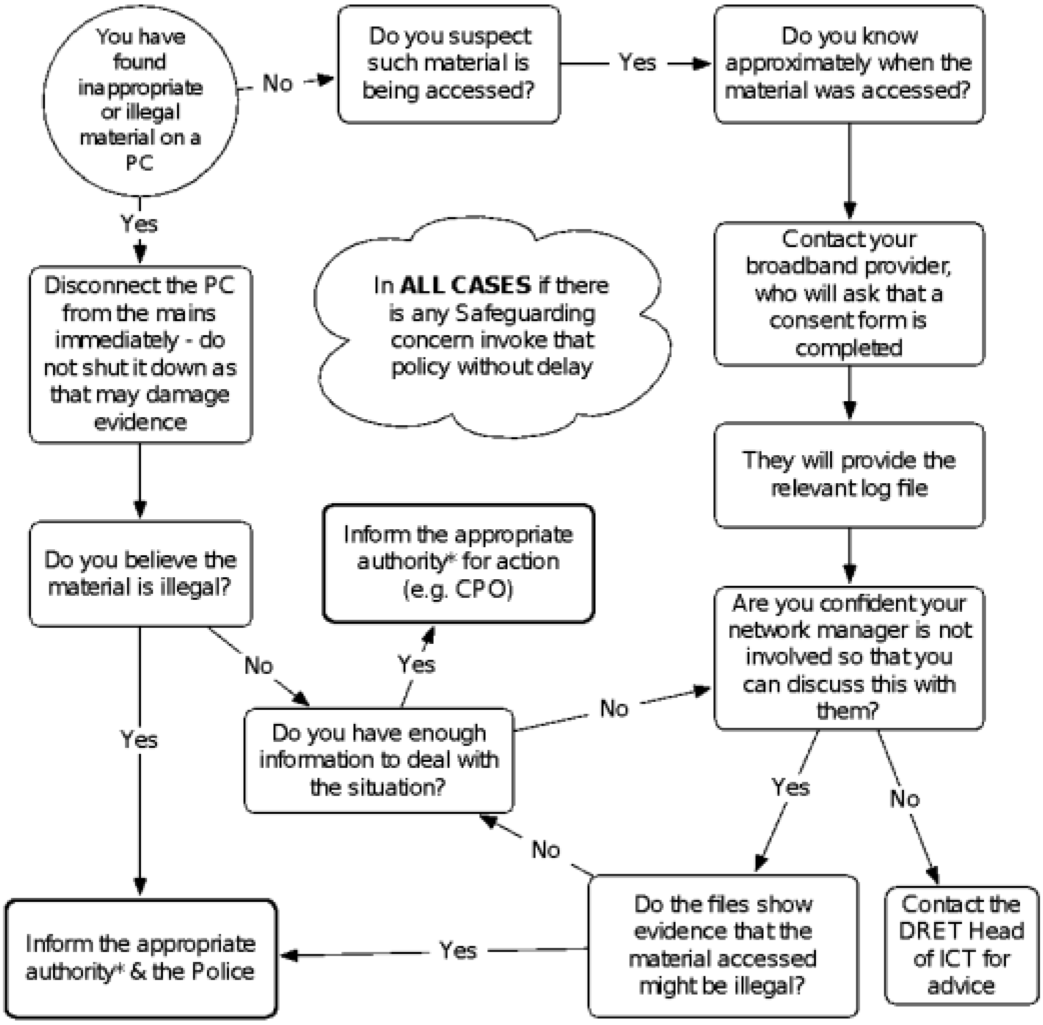
15.8 Responding to incidents of misuse

It is hoped that all members of the academy community will be responsible users of IT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse:

15.9 If any apparent or actual misuse appears to involve illegal activity ie.

- child sexual abuse images
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials

The following flow-chart must be followed. It is essential that Safeguarding procedures be invoked without delay where required.


You have found inappropriate or illegal material on a PC
No
Do you suspect such material is being accessed?
Yes
Do you know approximately when the material was accessed?
Yes
Disconnect the PC from the mains immediately - do not shut it down as that may damage evidence
In ALL CASES if there is any Safeguarding concern invoke that policy without delay
Contact your broadband provider, who will ask that a consent form is completed
They will provide the relevant log file
Do you believe the material is illegal?
Inform the appropriate authority* for action (e.g. CPO)
No
Yes
Are you confident your network manager is not involved so that you can discuss this with them?
No
Yes
Do you have enough information to deal with the situation?
Yes
No
No
Inform the appropriate authority* & the Police
Yes
Do the files show evidence that the material accessed might be illegal?
Contact the DRET Head of ICT for advice

*Appropriate authority will depend on the case. For any safeguarding issue it must be the Child Protection Officer who will then ensure the correct staff are involved. For any potential staff disciplinary issue it must be the Principal. Any issue concerning the Principal must be referred to the Trust CEO. Be aware of the Child Protection and Disciplinary policies in academy.

15.10 If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (as above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation.

15.11 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.

15.12 It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures.

15.13 This policy does not form part of any employee's contract of employment. The Trust may alter or adapt this policy, and any components of it, at any time provided it notifies the Chair of the Local Governing Bodies.

15.14 The Head of IT will review this policy at least every year and assess its implementation and effectiveness.