David Ross Education Trust
Broadening Horizons

E-SAFETY POLICY

Academy Name: **Lodge Park Academy**

Academy Logo:

Date: July 2017

Background / Rationale

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.

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.

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 should help to ensure safe and appropriate use. The development and implementation of such a strategy should involve all the stakeholders in a child's education from the principal and governors to the senior leaders and classroom teachers, support staff, parents, members of the community and the students themselves.

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.

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.

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).

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

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. ● Teachers uphold public trust in the profession and maintain high standards of ethics and behaviour, within and outside school, by: o treating students 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 students' well-being, in accordance with statutory provisions 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 students' 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.	See: ● Roles & responsibilities, teachers & support staff ● Education & training: staff ● Staff and volunteer acceptable use policy In addition … including in electronic communication of all kinds … applying safeguarding policy and procedure rigorously in the context of e-safety … including in electronic communication of all kinds

The 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.

Development / Monitoring / Review of this Policy

This e-safety policy has been developed by a working group made up of:

- *Academy E-Safety Coordinator / Officer:* ***Anne Franklin***
- *Headteacher / Senior Leaders:* ***Alison Hayes***
- *Teachers:* ***Andi York / Anne Franklin***
- *Support Staff*
- *ICT Technical staff:* ***Clare Curchin, Sean Everard***
- *Governors:* ***Andrew Corner***

Consultation with the whole academy community has taken place through the following:

- *Staff meetings*
- *Sub Committee Meeting*
- *Parents evening*
- *Academy website*
- *Student Council*

Schedule for Development / Monitoring / Review

This e-safety policy was approved by the *Finance and General Purposes on:*	*21st May 2014*
The implementation of this e-safety policy will be monitored by the:	*E-safety Co-ordinator* *Principal* *Business Manager*
Monitoring will take place at regular intervals:	*Annually*
The *Finance and General Purposes* 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:	*December 2016*
Should serious e-safety incidents take place, the following external persons / agencies should be informed:	*DRET Head of ICT, DRET Regional IT Manager, Safeguarding Officer, Police Commissioner's Office*

The academy will monitor the impact of the policy using:

- *Logs of reported incidents with E-safety officer*
- *Surveys / questionnaires of*
    - *students (eg Ofsted "Tell-us" survey / CEOP ThinkUknow survey)*
    - *parents / carers*
    - *staff*

Scope of the Policy

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 ICT systems, both in and out of academy.

The Education and Inspections Act 2006 empowers our Principal, 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.

The academy will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of academy.

Roles and Responsibilities

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

Governors:

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Finance and General Purposes Sub-Committee receiving regular information about e-safety incidents and monitoring reports. A member of the Governing Body has taken on the role of E-Safety Governor.

The role of the E-Safety Governor will include:

- *regular meetings with the E-Safety Co-ordinator / Officer*
- *regular monitoring of e-safety incident logs*
- *reporting to relevant Governors committee / meeting*

Principal and Senior Leaders:

- The Principal is responsible 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 is responsible for ensuring that the E-Safety Coordinator 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 academy will need to describe this and may wish to involve the Local Authority in this process)
- The Principal will receive termly reports from the E-safety Co-ordinator/Officer.
- **The Principal and 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.**

E-Safety Coordinator / Officer: Anne Franklin

- leads the e-safety working group
- 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 included in staff induction handbook.
- provides training and advice for staff
- liaises with the Local Authority and Trust staff
- liaises with academy ICT technical staff
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments
- meets regularly with E-Safety Governor to discuss current issues and review incident logs
- attends relevant meeting / committee of Governors
- reports regularly to the Principal

Network Manager / Technical staff: *Clare Curchin, Sean Everard*

The Business Manager / Network Managers are responsible for ensuring:

- that the academy's ICT 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
- 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 / Virtual Learning Environment (VLE) / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the E-Safety Co-ordinator and the Principal for investigation / action / sanction
- that monitoring software / systems are implemented and updated as agreed in academy policies

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 academy Staff Acceptable Use Policy / Agreement (AUP)
- they report any suspected misuse or problem to the E-Safety Co-ordinator / Officer and Principal for investigation / action / sanction

- digital communications with students (email / Virtual Learning Environment (VLE) / voice) 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, extracurricular and extended academy activities
- they are aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current academy 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

Designated person for child protection / Child Protection Officer

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

E-Safety Working Group

Members of the *E-safety committee* will assist the *E-Safety Coordinator, as above* with:

- the production / review / monitoring of the academy e-safety policy / documents.

Students:

- are responsible for using the academy ICT systems in accordance with the Student Acceptable Use Policy, which they will be expected to sign before being given access to academy systems.
- 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

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. In some cases parents and carers will not fully understand the issues and be less experienced in the use of ICT than their children.

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.

Parents and carers will be responsible for:

- endorsing (by signature) the Student Acceptable Use Policy
- accessing the academy website / VLE / on-line student records in accordance with the relevant academy Acceptable Use Policy.

Community Users

Community Users who access academy ICT 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.

Policy Statements

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.

E-Safety education will be provided in the following ways: (statements will need to be adapted, depending on the age of the *students* and the academy's structure)

- A planned e-safety programme will be provided as part of ICT / PHSE / other lessons 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 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
- Staff should act as good role models in their use of ICT, the internet and mobile devices

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 experiences. Parents often 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.

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

- Letters, newsletters, web site
- Parents evenings

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.
- 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 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 meetings..
- The E-Safety Coordinator will provide advice / guidance / training as required to individuals as required

Training – Governors

Governors should take part in e-safety training / awareness sessions, with particular importance for those who are members of any subcommittee / group involved in ICT / e-safety / health and safety / child protection. This may be offered in a number of ways:

- Participation in academy training / information sessions for staff or parents

Technical – infrastructure / equipment, filtering and monitoring

The academy will be responsible for ensuring that the academy infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities:

- Academy ICT 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 ICT systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to academy ICT systems. *Details of the access rights available to groups of users will be recorded by the Business Manager (or other person) and will be reviewed, at least annually, by the E-Safety Working Group.*
- All users (at KS2 and above) will be provided with a username and password by the Assistant Network Manager who will keep an up to date record of users and their usernames. Users will be required to change their password every 90 days.
- The “master / administrator” passwords for the academy ICT system, used by the Assistant Network Manager must also be available to the Business Manager and kept in a secure place (e.g. academy safe)
- The academy should never allow one user to have sole administrator access
- Users will be made 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.

- The academy maintains and supports the managed filtering service
    - The academy has provided enhanced user-level filtering through the use of the Watchguard filtering programme.
    - In the event of the Assistant Network Manager needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Business Manager.
    - Requests from staff for sites to be removed from the filtered list will be considered by the Assistant Network Manager and The Business Manager to ensure protection for the Assistant 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 logs of such actions shall be reviewed regularly by the E-Safety Governor
- Remote management tools are used by staff to control workstations and view users activity
- An appropriate system is in place (Impero) for users to report any actual / potential e-safety incident to the Assistant Network Manager.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc from accidental or malicious attempts which might threaten the security of the academy systems and data.
- An agreed policy is in place (Acceptable Use Policy) for the provision of temporary access of "guests" (e.g. trainee teachers, visitors) onto the academy system.
- An agreed policy is in place (Acceptable Use Policy) regarding the downloading of executable files by users
- An agreed policy is in place (Acceptable Use Policy) regarding the extent of personal use that users (staff / students /community users) and their family members are allowed on laptops and other portable devices that may be used out of academy.
- An agreed policy is in place (Acceptable Use Policy) that allows staff to / forbids staff from installing programmes on academy workstations / portable devices.
- An agreed policy is in place (Data Protection Policy) (eg memory sticks / CDs / DVDs) by users on academy workstations / portable devices.
- The academy infrastructure and individual workstations are protected by up to date virus software.
- Personal data cannot be sent over the internet or taken off the academy site unless safely encrypted or otherwise secured.

Curriculum

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages in the use of ICT 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.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs, discrimination) that would normally result

in internet searches being blocked. In such a situation, staff can request that the Assistant Network Manager 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.
- 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.

Use of digital and video images - Photographic, Video

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. There are many reported incidents of employers carrying 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 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.
- Written permission from parents or carers will be obtained before photographs of students are published on the academy website

Data Protection

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

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure

- Only transferred to others with adequate protection.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.
- When personal data is stored on any portable computer system, USB stick or any other removable media:
    - the data must be encrypted and password protected
    - the device must be password protected (many memory sticks / cards and other mobile devices cannot be password protected)
    - the device must offer approved virus and malware checking software
    - the data must be securely deleted from the device, in line with the Acceptable Use Policy once it has been transferred or its use is complete

Communications

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

	Staff & other adults				Students			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to academy	✓				✓			
Use of mobile phones in lessons		✓				✓		
Use of mobile phones in social time	✓				✓			
Taking photos on mobile phones or other camera devices		✓				✓		
Use of hand held devices eg PDAs, PSPs	✓					✓		
Use of personal email addresses in academy, or on academy network				✓				✓
Use of academy email for personal emails				✓				✓

Use of chat rooms / facilities				✓				✓
Use of instant messaging				✓				✓
Use of social networking sites				✓				✓
Use of blogs (personal)				✓				✓

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.
- 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.

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 ICT 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.

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:

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**					x
	promotion or conduct of illegal acts, eg under the child protection, obscenity, computer misuse and fraud legislation					x
	adult material that potentially breaches the Obscene Publications Act in the UK					x
	criminally racist material in UK					x
	pornography				x	
	promotion of any kind of discrimination				x	
	promotion of racial or religious hatred				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	
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by SWGfL and / or the academy					x	
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions					x	

Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)				x	
Creating or propagating computer viruses or other harmful files				x	
On-line gaming (educational)		✓			
On-line gaming (non-educational)					
On-line gambling					
On-line shopping / commerce					
File sharing					
Use of social networking sites					
Use of video broadcasting eg Youtube					

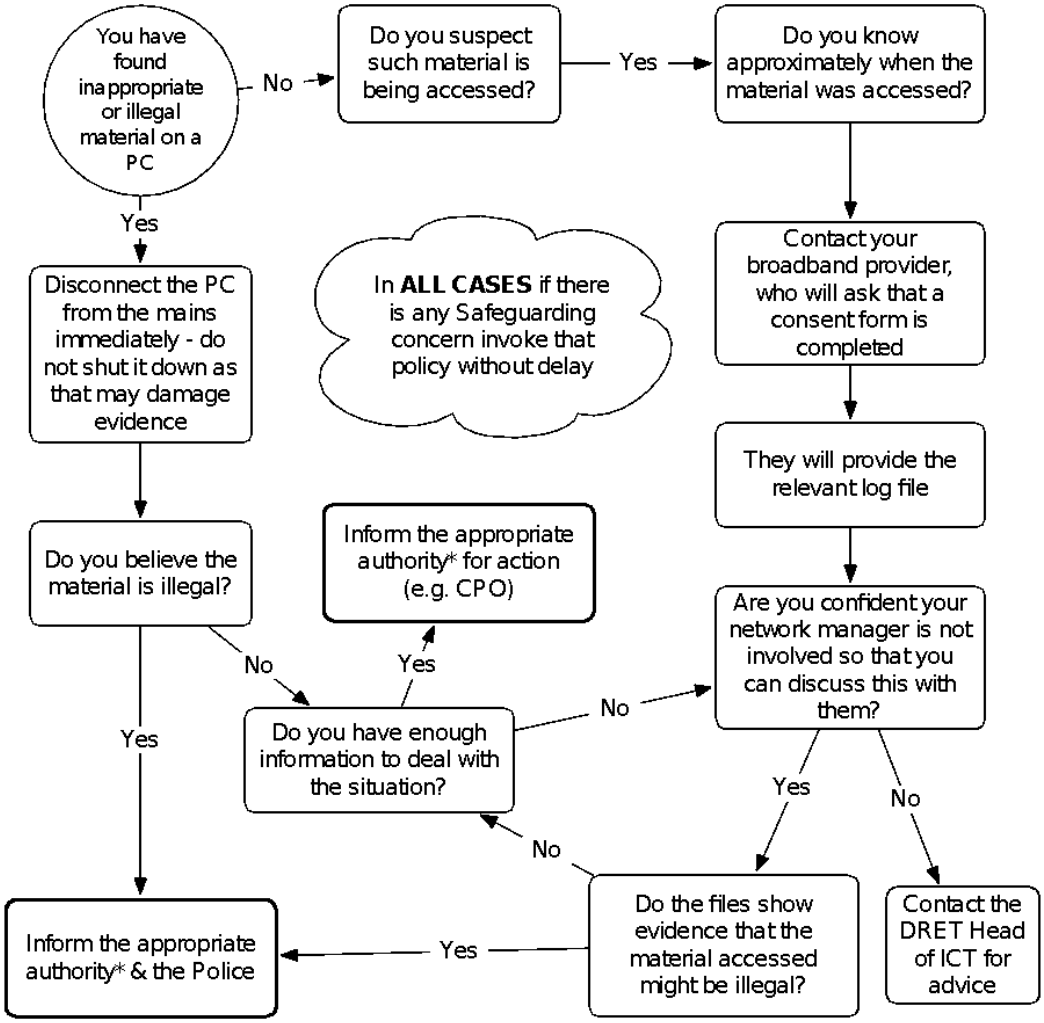
Responding to incidents of misuse

It is hoped that all members of the academy community will be responsible users of ICT, 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:

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 much be followed. It is essential that Safeguarding procedures be invoked without delay where required.



*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.

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.

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 - Appropriate sanctions will be taken after the incidents have been investigated. Parents will be informed as needed.

Students	Actions/Sanctions					
Incidents:	Refer to class teacher / tutor	Refer to House Manager	Refer to Principal	Refer to Police	Refer to technical support staff for action re filtering / security etc	Appropriate Sanctions
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 handheld device		✓				✓
Unauthorised use of social networking / instant messaging / personal email		✓				✓
Unauthorised downloading or uploading of files		✓				✓
Allowing others to access academy network by sharing username and passwords		✓			✓	✓
Attempting to access or accessing the academy network, using another student's / pupil's account		✓			✓	✓
Attempting to access or accessing the academy network, using the account of a member of staff		✓	✓		✓	✓
Corrupting or destroying the data of other users		✓				✓
Sending an email, text or instant 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 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		✓			✓	✓

Students	Actions/Sanctions					
Incidents:	Refer to line manager	Refer to Principal	Refer to Local Authority / DRET /HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc	Disciplinary action as appropriate, which might include warning or suspension
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	✓	✓	✓	✓	✓	✓
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email	✓	✓				✓
Unauthorised downloading or uploading of files	✓	✓				✓
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	✓	✓				✓
Careless use of personal data eg holding or transferring data in an insecure manner	✓					✓
Deliberate actions to breach data protection or network security rules	✓	✓				✓
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	✓	✓	✓			✓
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	✓	✓				✓
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students	✓	✓	✓			✓
Actions which could compromise the staff member's professional standing	✓	✓	✓			✓

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 filtering system	✓	✓			✓	✓
Accidentally accessing offensive or pornographic material and failing to report the incident	✓	✓	✓		✓	✓
Deliberately accessing or trying to access offensive or pornographic material	✓	✓	✓	✓	✓	✓
Breaching copyright or licensing regulations	✓	✓				✓
Continued infringements of the above, following previous warnings or sanctions	✓	✓	✓			

Student / Pupil Acceptable Use Policy Agreement

New technologies have become integral to the lives of children and young people in today's society, both within our academy and in their lives outside academy. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that academy ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

The academy will make every effort to ensure that students will have good access to ICT to enhance their learning and will, in return, expect the students to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use academy ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users.
For my own personal safety:

- I understand that the academy will monitor my use of the ICT systems, email and other digital communications.
- I will treat my username and password like my toothbrush – I will not share it, nor will I try to use any other person's username and password.

- I will be aware of “stranger danger”, when I am communicating on-line.
- I will not disclose or share personal information about myself or others when on-line.
- If I arrange to meet people off-line that I have communicated with on-line, I will do so in a public place and take an adult with me.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.
- I understand that everyone has equal rights to use technology as a resource and:
- I understand that the academy ICT systems are primarily intended for educational use and that I will not use the systems for personal or recreational use unless I have permission to do so.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.

I will act as I expect others to act toward me:

- I will respect others’ work and property and will not access, copy, remove or otherwise alter any other user’s files, without the owner’s knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.
- I recognise that the academy has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the academy:
- I will only use my personal hand held / external devices (mobile phones / USB devices etc.) within the allocated areas, at the allowed times. I understand that, if I do use my own devices in academy, I will follow the rules set out in this agreement, in the same way as if I was using academy equipment.
- I will only use chat and social networking sites on my own equipment with permission and at the times that are allowed
- I will not use ‘peer 2 peer’ file sharing, video broadcasting (e.g. YouTube), chat and social networking sites on school equipment, unless they are a requirement of my academic course and I have permission of a member of staff to do so or under supervision as part of a formal investigation.
- I will not access on-line gaming (except on formally allowed, educational sites), on-line gambling or internet shopping sites at any time whilst within the academy grounds, either on academy equipment or my own.
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others.
- I will not attempt to use any sites or software that might allow me to bypass the academy’s internet filtering and security systems.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any attachments to emails, unless I know and trust the person / organisation who sent the email, due to the risk of the attachment containing viruses or other harmful programmes.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings.

When using the internet for research or recreation, I recognise that:

- I should ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not try to download copies (including music and videos)
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.
- I understand that I am responsible for my actions, both in and out of academy:
- I understand that the academy also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of academy and where they involve my membership of the academy community (e.g. cyber-bullying, use of images or personal information).
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action.

Please complete the sections on the next page to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to academy ICT systems.

Student / Pupil Acceptable Use Agreement Form

This form relates to the student / pupil Acceptable Use Policy (AUP), to which it is attached. Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to academy ICT systems.

- I have read and understand the above and agree to follow these guidelines when:
- I use the academy ICT systems and equipment (both in and out of academy)
- I use my own equipment in academy (when allowed) eg mobile phones, PDAs, cameras etc
- I use my own equipment out of academy in a way that is related to me being a member of this academy eg communicating with other members of the academy, accessing academy email, VLE, website etc.

Name of Student / Pupil	
Group / Class	

Signed		Date	

Staff (and Volunteer) Acceptable Use Policy Agreement Template

New technologies have become integral to the lives of children and young people in today's society, both within academies and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that academy ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of ICT in their everyday work.
- The academy will try to ensure that staff and volunteers will have good access to ICT to enhance their work, to enhance learning opportunities for students learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use academy ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that students receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed e-safety in my work with young people.

For my professional and personal safety:

- I understand that the academy will monitor my use of the ICT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of academy ICT systems (e.g. laptops, email, VLE etc.) outside of the academy, in addition to any other policies and agreements relating to specific equipment and systems (e.g. The LPA Laptop/Mobile Device Agreement).
- I understand that the academy ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use, including personal email account access, chat and social media in my own time, such as during designated breaks and after hours and only provided that the security and filtering systems allow it.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using academy ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission except as a last resort in exceptional circumstances such as

student absence on coursework deadline day or affecting group work. This access must only be granted by the IT Support Team.

- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the academy's policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the academy website / VLE) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only communicate with students and parents / carers using official academy systems. Any such communication will be professional in tone and manner. I will not disclose my personal telephone numbers, email addresses, social media accounts or any other personal contact details to students or their parents / carers or enter into any kind of dialog with them if contacted via those methods.
- I will not engage in any on-line activity that may compromise my professional responsibilities.
- The academy and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the academy:
- When I use my personal hand held / external devices (PDAs / laptops / mobile phones / USB devices etc.) in the academy, I will follow the rules set out in this agreement, in the same way as if I was using academy equipment. I will also follow any additional rules set by the academy about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
- I will store my data on the academies servers to ensure that it is backed up regularly. I will take responsibility for making my own regular backups of any data I am unable to store in this way.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in academy policies, nor will I attempt to circumvent any security measures that have been put in place to prevent these actions.
- I will not disable or cause any damage to academy equipment, or the equipment belonging to others.

- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the Data Protection Policy (or other relevant academy policy). Where personal data is transferred outside the secure academy network, it must be encrypted.
- I understand that data protection policy requires that any staff or student / pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by academy policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for academy sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of academy:

- I understand that this Acceptable Use Policy applies not only to my work and use of academy ICT equipment in academy, but also applies to my use of academy ICT systems and equipment out of academy and my use of personal equipment in academy or in situations related to my employment by the academy.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action.

I have read and understand the above and agree to use the academy ICT systems (both in and out of academy) and my own devices (in academy and when carrying out communications related to the academy) within these guidelines.

Staff / Volunteer Name

Signed

Date

Parent / Carer Acceptable Use Policy Agreement Template

The academy will try to ensure that students will have good access to ICT to enhance their learning and will, in return, expect the students to agree to be responsible users.

A copy of the Student / Pupil Acceptable Use Policy is attached to this permission form, so that parents / carers will be aware of the academy expectations of the young people in their care.
Parents are requested to sign the permission form below to show their support of the academy in this important aspect of the academy's work.

Permission Form

Parent / Carers Name

Student / Pupil Name

As the parent / carer of the above students, I give permission for my son / daughter to have access to the internet and to ICT systems at academy.

I know that my son / daughter has signed an Acceptable Use Agreement and has received, or will receive, e-safety education to help them understand the importance of safe use of ICT – both in and out of academy.

I understand that the academy will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems. I also understand that the academy cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my son's / daughter's activity on the ICT systems will be monitored and that the academy will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the academy if I have concerns over my child's e-safety.

Signed

Date

Use of Digital / Video Images

The use of digital / video images plays an important part in learning activities. Students and members of staff may use digital cameras to record evidence of activities in lessons and out of academy. These images may then be used in presentations in subsequent lessons. Images may also be used to celebrate success through their publication in newsletters, on the academy website and occasionally in the public media.

The academy will comply with the Data Protection Act and request parents / carers permission before taking images of members of the academy. We will also ensure that when images are published that the young people cannot be identified by the use of their names.

Parents are requested to sign the permission form below to allow the academy to take and use images of their children in the ways described. Please note, however, that the academy has a legal obligation to hold an image of each of its students in its internal data management systems for purposes of identification, which is updated annually.

Permission Form

Parent / Carers Name	
Student / Pupil Name	

As the parent / carer of the above *student / pupil*, I agree to the academy taking and using digital / video images of my child / children. I understand that the images will only be used to support learning activities or in publicity that reasonably celebrates success and promotes the work of the academy.

I agree that if I take digital or video images at, or of, – academy events which include images of children, other than my own, I will abide by these guidelines in my use of these images.

Signed		Date	

Academy Password Security

The academy will be responsible for ensuring that the *academy infrastructure / network* is as safe and secure as is reasonably possible and that:

- users can only access data to which they have right of access
- no user should be able to access another's files, without permission (or as allowed for monitoring purposes within the academy's policies).
- access to personal data is securely controlled in line with the academy's data protection policy
- logs are maintained of access by users and of their actions while users of the system

A safe and secure username / password system is essential if the above is to be established and will apply to all academy ICT systems, including email and Virtual Learning Environment (VLE).

Responsibilities

The management of the password security policy will be the responsibility of the Assistant Network Managers.

All users (adults and young people) will have responsibility 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.

Passwords for new users, and replacement passwords for existing users can be allocated by members of the IT Support Team

Staff users will change their passwords every 90 days.

Training / Awareness

It is essential that users should be made aware of the need for keeping passwords secure, and the risks attached to unauthorised access / data loss. This should apply to even the youngest of users, even if class log-ons are being used.

Members of staff will be made aware of the academy's password policy:

- at induction
- through the academy's e-safety policy and password security policy
- through the Acceptable Use Agreement
- Students will be made aware of the academy's password policy:
- in ICT and / or e-safety lessons (the academy should describe how this will take place)
- through the Acceptable Use Agreement

In the event of a serious security incident, the police may request and will be allowed access to passwords used for encryption. Auditors also have the right of access to passwords for audit investigation purposes

User lists, IDs and other security related information must be given the highest security classification and stored in a secure manner.

Data Handling

This section sets out the procedures for proper handling of data and complements the Data Protection Policy.

The Academy will do everything within its power to ensure the safety and security of any material of a personal or sensitive nature.

It is the responsibility of all members of the academy community to take care when handling, using or transferring personal data that it cannot be accessed by anyone who does not:

- have permission to access that data
- need to have access to that data.

All transfer of data is subject to risk of loss or contamination.

The academy will ensure that ICT systems are set up so that the existence of protected files is hidden from unauthorised users and that users will be assigned a clearance that will determine which files are accessible to them.

All users will be given secure user names and strong password policy will be enforced. Staff Users will be obliged to change their network logon passwords every 90 days. User names and passwords must never be shared.

Personal data may only be accessed on machines that are securely password protected. Any device that can be used to access data must be locked if left (even for very short periods). The storage on the network and on the machine must be encrypted.

All storage media must be stored in an appropriately secure and safe environment that avoids physical risk, loss or electronic degradation.

Private equipment must never be used to store personal data.

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

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

Storage on removable media is prohibited except in the case of encrypted backups. Removable media may be used to transfer data out of the academy as described below.

Secure transfer of data and access out of academy

The academy recognises that personal data may be accessed by users out of academy, or transferred to the Trust or other agencies. In these circumstances:

Users may not remove or copy sensitive or personal data from the academy or authorised premises without permission and unless the media is encrypted and password protected and is transported securely for storage in a secure location.

- Users must take particular care that computers or removable devices which contain personal data must not be accessed by other users (eg family members) when out of academy.
- When data is required by an authorised user from outside the academy premises (for example, by a teacher or student working from their home or a contractor) they must have secure remote access to the management information system (MIS) or learning platform.
- Users must protect all portable and mobile devices, including media, used to store and transmit personal information using approved encryption software.
- Particular care should be taken if data is taken or transferred to another country, particularly outside Europe, and advice should be taken from the local authority in this event.

Disposal of data

The disposal of protected data, in either paper or electronic form, must be conducted in a way that makes reconstruction highly unlikely. Electronic files must be securely overwritten, in accordance with government guidance, and other media must be shredded, incinerated or otherwise disintegrated for data.

Academy Filtering

Responsibilities

The responsibility for the management of the school's filtering policy will be held by the Business Manager, Assistant Network Managers and DRET Regional IT Manager.
They will manage the school filtering, in line with this policy and will keep records / logs of changes and of breaches of the filtering systems.

To ensure that there is a system of checks and balances and to protect those responsible, changes to the filtering service must:

- **be logged**

All users have a responsibility to report immediately to the IT Support Team any infringements of the school's filtering policy of which they become aware or any sites that are accessed, which they believe should have been filtered.

Users must not attempt to use any programs or software that might allow them to bypass the filtering / security systems in place to prevent access to such materials.

Education / Training / Awareness

Students will be made aware of the importance of filtering systems through the e-safety education programme. They will also be warned of the consequences of attempting to subvert the filtering system.

Staff users will be made aware of the filtering systems through: (amend as relevant)

- signing the AUP
- induction training

Parents will be informed of the school's filtering policy through the Acceptable Use agreement and through e-safety awareness sessions / newsletter etc. (amend as relevant)

Changes to the Filtering System

Requests for changes to the academy's filtering system must be made by members of staff, by email to the Assistant Network Managers. Changes will be at the discretion of the responsible member of staff who will log changes as described above. The E-Safety Governor will act as a check on the changes being made and raise any concerns through the E-Safety Working Group.

Users who gain access to, or have knowledge of others being able to access, sites which they feel should be filtered (or unfiltered) should report this in the first instance to Assistant Network Manager who will decide whether to make school level changes (as above).

Monitoring

No filtering system can guarantee 100% protection against access to unsuitable sites. The academy will therefore monitor the activities of users on its network and on academy equipment as indicated in the E-Safety Policy and the Acceptable Use agreement.