Overdale Junior School

E-SAFETY POLICY

January 2019

Next Policy Review: January 2020

Background / Rationale

New technologies have become integral to the lives of children and young people in today's society, both our school 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 pupils 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 school 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 headteacher and governors to the senior leaders and classroom teachers, support staff, parents, members of the community and the pupils themselves.

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

However, the use of these new technologies can put young people at risk within and outside the school. 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 school 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 pupils 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 pupils. 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:
  ○ treating pupils with dignity, building relationships rooted in mutual respect, and at all times observing proper boundaries appropriate to a teacher's professional position
  ○ having regard for the need to safeguard pupils' well-being, in accordance with statutory provisions
  ○ 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.
	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 school 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 guardians 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 staff within the school, which include

- ICT subject coordinator
- SLT
- Health and safety officer
- School technician
- Responses from our school community.

Consultation with the whole school community has taken place through staff meetings. This policy will be updated annually, or in the event that requires it to be updated.

Schedule for Development / Monitoring / Review

This e-safety policy was approved by the Health and safety officer on*:*	*October 2018*
The implementation of this e-safety policy will be monitored by the:	Jordan Cross as ICT coordinator Matthew Evans as Health and safety officer.
Monitoring will take place at regular intervals:	At least annually.
The Head teacher 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, or when amended.
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:	October 2019
Should serious e-safety incidents take place, the following external persons / agencies should be informed:	Juliet Hart as Head teacher Matthew Evans as health and safety officer. Police

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited) provided by the ICT Coordinator for a time period specified by the reviewer
- Internal monitoring data for network activity

Scope of the Policy

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

The Education and Inspections Act 2006 empowers our Head teacher, to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the school 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 school, but is linked to membership of the school.

The school 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 school.

Roles and Responsibilities

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

Governors:

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors, receiving regular information about e-safety incidents and monitoring reports. A committee of Governors are taking 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
- regular monitoring of filtering / change control logs
- reporting to relevant Governors committee / meeting

Head teacher and Senior Leaders:

- The Head teacher is responsible for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to the E-Safety Co-ordinator.
- The Head teacher / Senior Leaders are responsible for ensuring that 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 Head teacher / Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school 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 annual monitoring reports from the E-Safety Co-ordinator.
- The Head teacher and another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.

E-Safety Coordinator / Officer:

- 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 school e-safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- provides training and advice for staff
- liaises with the Local Authority and Trust staff
- liaises with school 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, review incident logs and filtering / change control logs
- attends relevant meeting of Governors
- reports regularly to Senior Leadership Team

Network Manager / Technical staff:

The ICT Technician and ICT Co-ordinator are responsible for ensuring:

- that the school's ICT infrastructure is secure and is not open to misuse or malicious attack
- that users may only access the school'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 school's filtering policy is applied and updated on a regular basis (see section on filtering)
- 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 / email is regularly monitored in order that any misuse or attempted misuse can be reported to the E-Safety Co-ordinator / Officer /Head teacher / Senior Leader / Head of ICT / ICT Co-ordinator.
- that monitoring software and systems are implemented and updated as agreed in school 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 school e-safety policy and practices
- they have read, understood and signed the school Staff Acceptable Use Policy
- they report any suspected misuse or problem
- digital communications with should be on a professional level and only carried out using official school systems

- e-safety issues are embedded in all aspects of the curriculum and other school activities
- pupils understand and follow the school e-safety and acceptable use policy
- pupils 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 school 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 school policies with regard to these devices
- in lessons where internet use is pre-planned students / pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Designated Safeguarding Lead:

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) with:

- the production / review / monitoring of the school e-safety policy.

Pupils:

- are responsible for using the school ICT systems in accordance with the Pupil Acceptable Use Policy, which they will be expected to sign before being given access to school 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 school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school 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 school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school

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 school will therefore take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and conversations.

Parents and carers will be responsible for:

- being aware of the Pupil Acceptable Use Policy via the school website
- adopting the e-safety policy of the school when using school associated communications.

Policy Statements

Education – pupils

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

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

- A planned e-safety programme will be provided as part of ICT or PHSE lessons and should be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school
- Key e-safety messages will be reinforced as part of a planned programme of assemblies
- Pupils will be taught in all lessons to be critically aware of the materials and content they access on-line and be guided to validate the accuracy of information
- Pupils should be helped to understand and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school
- Pupils 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 ICT systems or 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

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 regularly.
- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Policies
- The E-Safety Coordinator (or other nominated person) will receive regular updates through attendance at training sessions and by reviewing guidance documents released by appropriate bodies.

Training – Governors

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

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

Technical – infrastructure / equipment, filtering and monitoring

The school will be responsible for ensuring that the school 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:

- School ICT systems will be managed in ways that ensure that the school 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 school ICT systems
- Servers, wireless systems and cabling must be securely located and physical access restricted

- All users will have clearly defined access rights to school ICT 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.
- All users will be provided with a username and password by Adam Lapidge.
- The "master / administrator" passwords for the school ICT system, used by the Network Manager (or other person) must also be available to the Head teacher or other nominated senior leader Matt Evans and ICT coordinator Jordan Cross.
- The school 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 school maintains and supports the managed filtering service provided by their broadband provider
    - In the event of the Network Manager (or other person) 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 Head teacher (or other nominated senior leader).
    - Any filtering issues should be reported immediately to the broadband provider.
    - Requests from staff for sites to be removed from the filtered list will be considered by the Network Manager and (Matt Evans) (nb an additional person should be nominated – 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 logs of such actions shall be reviewed regularly by the E-Safety Governor
- School ICT technical staff regularly monitor and record the activity of users on the school ICT systems and users are made aware of this in the Acceptable Use Policy.
- An appropriate system is in place (email sent to key personnel) for users to report any actual / potential e-safety incident to the Network Manager (or other relevant person).
- Appropriate security measures are in place (schools may wish to provide more detail) 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 school systems and data.
- An agreed policy is in place (to be described) for the provision of temporary access of "guests" (eg trainee teachers, visitors) onto the school system.
- An agreed policy is in place (to be described) regarding the downloading of executable files by users – programs installed by Network Manager.
- An agreed policy is in place (to be described) regarding the extent of personal use that users (staff / students / pupils / community users) and their family members are

allowed on laptops and other portable devices that may be used out of school. (see School Personal Data section for further detail)

- An agreed policy is in place (to be described) that allows staff to / forbids staff from installing programmes on school workstations / portable devices.
- An agreed policy is in place (to be described) regarding the use of removable media (eg memory sticks / CDs / DVDs) by users on school workstations / portable devices. (see School Personal Data section for further detail) – USBs must be encrypted only when necessary.
- The school infrastructure and individual workstations are protected by up to date virus software.
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured. (see School Personal Data section for further detail)

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 / pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.*
- *Where students / pupils are allowed to freely search the internet, 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 Network Manager (and other relevant person) can temporarily remove those sites from the filtered list for the period of study.. Any request to do so, should be auditable, with clear reasons for the need.*
- *Students / pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information*
- *Students / pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.*

Use of digital and video images - Photographic, Video

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff and pupils 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 school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate students / pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet eg on social networking sites.
- Staff are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that students / pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include students / pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website (may be covered as part of the AUP signed by parents or carers at the start of the year see Parents / Carers AUP Agreement)
- Pupil's work can only be published with the permission of the pupil and parents or carers.

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 school policy (below) once it has been transferred or its use is complete

- (The school will need to set its own policy as to whether data storage on removal media is allowed, even if encrypted – some organisations do not allow storage of personal data on removable devices.)

Communications

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

	Staff & other adults				Students / Pupils			
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 school	X							X
Use of mobile phones in lessons				X				X
Use of mobile phones in lessons in an emergency – call for assistance	X							
Use of mobile phones in social time – in the staff room	X							X
Use of mobile phone in classes even when pupils are not around				X				
Taking photos on mobile phones of pupils at anytime				X				X
Taking photos of pupils work whilst in the staff room or at home	X							
Taking photos on school ipads and devices	X						X	
Use of personal email addresses in school, or on school network		X						X
Use of school email for personal emails				X				X
Use of school email addresses on personal phones. But can only be	X							

checked or emails sent in the staff room or at home.								
Use of chat rooms / facilities with any pupil or parent				X				X
Use of instant messaging with any pupil or parent				X				X
Use of social networking sites for school purposes – Twitter. To be updated during school time on the school laptops or ipads. At Home staff can update Twitter with their phones.	X							x
Use of blogs for school purposes	x							X

When using communication technologies the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school 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 school 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 / pupils or parents / carers (email, chat, VLE etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or public chat / social networking programmes must not be used for these communications.
- pupils 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 school 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 school 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 a school context, either because of the age of the users or the nature of those activities.

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

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 school or brings the school into disrepute				x	
Using school 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 school					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	

Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet					
On-line gaming (educational)		X			
On-line gaming (non educational)				X	
On-line gambling				X	
On-line shopping / commerce				X	
File sharing				X	
Use of social networking sites	X				
Use of video broadcasting eg Youtube			X		

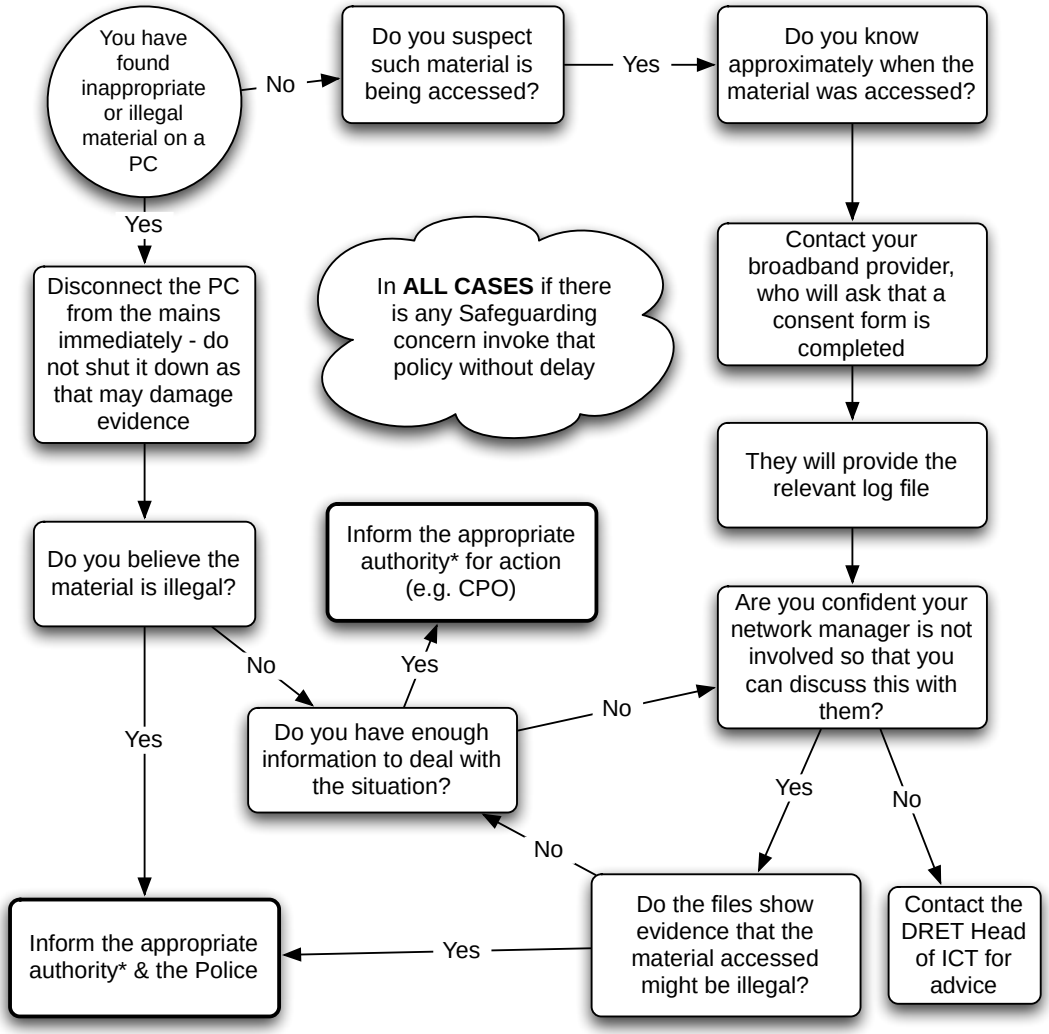
Responding to incidents of misuse

It is hoped that all members of the school 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 school 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.

Pupils Actions / Sanctions

Incidents:	Refer to class teacher / tutor	Refer to Head of Department / Head of Year / other	Refer to Head teacher	Refer to Police	Refer to technical support staff for action re filtering / security etc	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction eg detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		x	x	x					
Unauthorised use of non-educational sites during lessons					x				
Unauthorised use of mobile phone / digital camera / other handheld device	X		x			X			
Unauthorised use of social networking / instant messaging / personal email	X		X		X	x			
Unauthorised downloading or uploading of files					x	x			
Allowing others to access school network by sharing username and passwords			x		X	x	x		
Attempting to access or accessing the school network, using another student's / pupil's account	X								
Attempting to access or accessing the school network, using the account of a member of staff		x					X		
Corrupting or destroying the data of other users		x					X		
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature		x							

Staff Actions / Sanctions

Incidents:	Refer to line managerr	Refer to Head teacher	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		x	x	x				
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email	X							
Unauthorised downloading or uploading of files	x				X			
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	x				x	X		
Careless use of personal data eg holding or transferring data in an insecure manner	X							
Deliberate actions to breach data protection or network security rules		x			x	X		
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	x	X		X				
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature		X		X				
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils		X		X				
Actions which could compromise the staff member's professional standing	x	X						

Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	x	X						
Using proxy sites or other means to subvert the school's filtering system	x	X						
Accidentally accessing offensive or pornographic material and failing to report the incident	x	x			X			
Deliberately accessing or trying to access offensive or pornographic material		X		X				
Breaching copyright or licensing regulations		X						
Continued infringements of the above, following previous warnings or sanctions		x						

Sexting

This policy uses this term as a description of a child under the age of 18 creating and sharing images to peers, also under 18. Due to the case of those involved being minors this is classed separately to abuse, and falls in to school safeguarding policies. Images or videos can range from semi-nude or suggestive to sexually explicit or nude.

Initial response to such activity:

All incidents involving youth produced sexual imagery should be responded to in line with the school's safeguarding and child protection policy.
When an incident involving youth produced sexual imagery comes to a school or college's attention:

• The incident should be referred to the DSL as soon as possible
• The DSL should hold an initial review meeting with appropriate school staff
• There should be subsequent interviews with the young people involved (if appropriate)
• Parents should be informed at an early stage and involved in the process unless there is good reason to believe that involving parents would put the young person at risk of harm
• At any point in the process if there is a concern a young person has been harmed or is at risk of harm a referral should be made to children's social care and/or the police immediately.

Disclosures

Disclosures about youth produced sexual imagery can happen in a variety of ways. The young person affected may inform a class teacher, the DSL in school, or any member of the school staff. They may report through an existing reporting structure, or a friend or parent may inform someone in school or college, or inform the police directly.
All members of staff (including non-teaching) should be made aware of how to recognise and refer any disclosures of incidents involving youth produced sexual imagery. This should be covered within staff training and within the school or college's child protection policy. Annex F contains a training exercise which may be used to highlight the issues for staff.
Any direct disclosure by a young person should be taken very seriously. A young person who discloses they are the subject of sexual imagery is likely to be embarrassed and worried about the consequences. It is likely that disclosure in school is a last resort and they may have already tried to resolve the issue themselves.

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 school 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. 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 school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

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

Acceptable Use Policy Agreement

I understand that I must use school 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 school 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 school 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 not use the school ICT systems for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (eg YouTube), unless I have permission of a member of staff to do so.

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 school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the school:
- I will NOT use my personal mobile phone or ipad in school. I understand that, if I do use my own devices in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.
- 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, nor will I 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 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 programs on a computer, nor will I try to alter computer settings.
- I will only use programs and messaging services provided by the school with permission and at the times that are allowed

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 school:
- I understand that the school 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 school and where they involve my membership of the school community (examples would be 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 school 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 school ICT systems.

- I have read and understand the above and agree to follow these guidelines when:
- I use the school ICT systems and equipment (both in and out of school)
- I will not use my own equipment in school eg mobile phones, iPads, cameras etc

Class:			Date:	
Name	Signed		Name	Signed

Staff (and Volunteer) Acceptable Use Policy Agreement

New technologies have become integral to the lives of children and young people in today's society, both within schools 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 school 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 school will try to ensure that staff and volunteers will have good access to ICT to enhance their work, to enhance learning opportunities for *students / pupils* 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 school 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 / pupils 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 school 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 school ICT systems (eg laptops) out of school.
- I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- 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 school ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- 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 school'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 (eg on the school website / VLE) it will not be possible to identify by name, or other personal information, those who are featured.

- I will only use chat and social networking sites in school in accordance with the school's policies.
- I will only communicate with pupils and parents using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.
- The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:
- When I use my personal hand held / external devices (PDAs / laptops / mobile phones / USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school 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 can use personal email addresses on the school ICT systems but during break times and will check for viruses and be password protected.
- 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 ensure that my data is regularly backed up, in accordance with relevant school policies.
- 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 school policies.
- I will not disable or cause any damage to school 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 school policy). Where personal data is transferred outside the secure school 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 school 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 school 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 school:

- I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment out of school and my use of personal equipment in school or in situations related to my employment by the school.
- 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 school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

STAFF			Date:	
Name	Signed		Name	Signed

Photographs and filming of pupils and use on the website and social media

Parents will be asked for their permission for their children's pictures to be taken and to be filmed. They will also be asked if these images can be used on any website or social media sites.

School Password Security

The school will be responsible for ensuring that the school infrastructure and 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 school's policies).
- access to personal data is securely controlled in line with the school'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 school ICT systems, including email and Virtual Learning Environment (VLE).

Responsibilities

The management of the password security policy will be the responsibility of *the* health and safety officer.

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. In most cases, pupils will be able to access the school system through a generic year log in. Staff are to use their login details provided by the school IT technician.

Passwords for new users, and replacement passwords for existing users can be allocated by the ICT technician, or with their consent.

Any changes carried out must be notified to the manager of the password security policy (above).

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 school's password policy:

- at induction
- through the school's e-safety policy and password security policy
- through the Acceptable Use Agreement
- students will be made aware of the school's password policy:
- in ICT and / or e-safety lessons (the school 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 School 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 school 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 school 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 passwords, which must be changed regularly. 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) and set to auto lock if not used for five minutes. 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 school 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 school as described below.

Secure transfer of data and access out of school

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

Users may not remove or copy sensitive or personal data from the school 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 school.
- When data is required by an authorised user from outside the school 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.

A Destruction Log should be kept of all data that is disposed of. The log should include the document ID, classification, date of destruction, method and authorisation.

Audit Logging / Reporting / Incident Handling

The activities of data users, in respect of electronically held personal information, will be logged and these logs will be monitored by responsible individuals.

These audit logs will be kept to provide evidence of accidental or deliberate security breaches – including loss of protected data or breaches of an acceptable use policy, for example.

Specific security events should be archived and retained at evidential quality for seven years.

The school has a policy for reporting, managing and recovering from information risk incidents, which establishes: (schools should determine their own reporting policy, in line with that of their LA, and add details here)

- a “responsible person” for each incident
- a communications plan, including escalation procedures
- and results in a plan of action for rapid resolution and
- a plan of action of non-recurrence and further awareness raising.

All significant data protection incidents must be reported as described in the Data Protection Policy to the Information Commissioner’s Office.

School Filtering

Responsibilities
The responsibility for the management of the school's filtering policy will be held by the ICT technician and e-safety coordinator.

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
- be reported to the E-Safety Governor every term in the form of an audit of the change control logs

All users have a responsibility to report immediately to Ross Lauder 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
Pupils / 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 school's filtering system must be made by members of staff, by email to Matt Evans. 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 Matt Evans 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 school will therefore monitor the activities of users on its network and on school equipment as indicated in the E-Safety Policy and the Acceptable Use agreement.