An Daras
Multi Academy Trust

An Daras Multi Academy Trust

On-Line Safety Policy

The An Daras Multi Academy Trust (ADMAT) Company

An Exempt Charity Limited by Guarantee

Company Number/08156955

Status: **Approved**	
Version	V1.1
Adopted	**Jan 19**
Adopted/Approved	**30 Jan 2019**
Next Review	**Feb 2021**
Advisory Committee	ADMAT Resources, Staffing and Safeguarding Committee
Linked Documents and Policies	School Computing Policy/Scheme of Learning ADMAT Acceptable Use of IT Policy School Behaviour Policy ADMAT Child Protection and Safeguarding Policy ADMAT Anti Bullying Policy ADMAT GDPR Policy ADMAT Staff Code of Conduct Policy ADMAT Use of Images Policy

An Daras Multi Academy Trust

On-Line Safety Policy

Background/Rationale

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 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 schools are bound. The MAT/school On-line 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 School Leaders and Local Governors to the Key Stage 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
- risk of being subject to grooming by those with whom they make contact on the internet
- 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
- inability to evaluate the quality, accuracy and relevance of information on the internet
- plagiarism and copyright infringement
- illegal downloading of music or video files
- 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 On-line Safety Policy is used in conjunction with other MAT/school policies (e.g. Behaviour, Anti-Bullying and Child Protection Policies, Acceptable Use, GDPR).

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 these risks.

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 On-line 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 On-line Safety Policy has been developed primarily by the MAT, Senior Leaders, IT Leaders and the Local Governing Body but all the groups below have played a part:

- Child Protection Officer
- Head of School/Senior Leaders
- teachers
- support Staff
- IT Technical staff
- Local Governors
- parents and carers
- community users

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

- staff meetings
- school Council
- Local Governors meeting
- school website

Schedule for Development/Monitoring/Review

This On-line Safety Policy approved by the MAT Board of Directors on:	Feb 2019
The implementation of this On-line Safety Policy will be monitored by the:	RSS Committee, LGAB , Senior Leadership Team, ADMAT Child Protection Officer
Monitoring will take place at regular intervals:	Every two years
Local Governing Body will receive a regular report on the implementation of the On-line Safety Policy (which will include anonymous details of on-line safety incidents) at regular intervals:	At least annually
On-line Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new digital or on-line threats or incidents that have taken place. The next anticipated review date will be:	Feb 2021
Should serious on-line safety incidents take place, the following external persons/ agencies should be informed:	ADMAT IT Manager, ADMAT Safeguarding Officer, Police Commissioner's Office

The school will monitor the impact of the On-line Safety Policy using:

- logs of reported incidents
- MAT internet service providers monitoring logs of internet activity (including sites visited)
- internal monitoring data for network activity
- surveys /questionnaires of;
  - ✓ pupils (e.g. Ofsted "Tell-us" survey / CEOP Think-U-know survey)
  - ✓ parents / carers
  - ✓ staff

Scope of the Policy

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

The Education and Inspections Act 2006 empowers Head Teachers/Head of Schools, to such extent as is reasonable, to regulate the behaviour of 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 on-line incidents covered by this policy, which may take place out of school, but is linked to membership of the MAT or school community.

The MAT or 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 on-line behaviour that take place out of school.

Roles and Responsibilities

The following section outlines the roles and responsibilities for on-line safety of individuals and groups within the MAT/school:

Local Governors: Governors are responsible for the monitoring and implementation of the of the On-line Policy by senior school staff. This will be carried out by the Local Governors receiving regular information about on-line incidents and monitoring reports. A member of the Local Governing Body must take on the role of On-line Safety/Safeguarding Governor. The role of will include;

- regular meetings with the on-line safety/DSL
- regular monitoring of on-line incident logs
- regular monitoring of filtering/change control logs
- reporting to relevant Local Governor meeting

Head Teachers/Head of School and Senior Leaders: The Head Teacher/Head of School is responsible for ensuring the safety (including on-line) of members of the individual school community, though the day to day responsibility for on-line safety may be delegated to the IT Leader;

- Head Teacher/Head of School/Senior Leaders are responsible for ensuring that the on-line safety/IT Leader and other relevant staff receive suitable CPD to enable them to carry out their safety roles and to train other colleagues, as relevant
- Head Teacher/Head of School/Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in individual schools who carry out the internal on-line safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles
- Senior Leadership Team will receive regular monitoring updates from the on-line/IT Leader

- Head Teacher/Head of School and another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious on-line safety allegation being made against a member of staff

On-line Safety/IT Leader: Takes day to day responsibility for on-line safety issues and has a leading role in implementing this safety policy/documents;

- ensures that all staff are aware of the procedures that need to be followed in the event of an on-line safety incident taking place
- provides training and advice for school staff
- liaises with the MAT IT service providers should the need arise
- liaises with school IT technical staff
- receives reports of on-line safety incidents and creates a log of incidents to inform future on-line safety developments,
- meets regularly with On-line Safety Local Governor to discuss current issues, review incident logs and filtering/change control logs
- attends relevant meetings of Local Governors
- reports regularly to Senior Leadership Team

MAT Network Manager/Technical Staff: MAT IT Technician/IT Service provider is responsible for ensuring;

- all MAT school's IT infrastructure is secure and is not open to misuse or malicious attack
- school meets the on-line safety technical requirements outlined in the Security Policy and Acceptable Usage Policy and any relevant MAT policy and guidance
- users may only access the MAT/school's networks through a properly enforced password protection policy, in which passwords are regularly changed
- MAT Central Office is informed of issues relating to the filtering applied by IT Service Provider
- MAT/school's filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- MAT IT Service Provider staff keep up to date with on-line safety technical information in order to effectively carry out their on-line safety role and to inform and update others as relevant
- use of the network/remote access/email is regularly monitored in order that any misuse/attempted misuse can be reported to the on-line safety Leader/Head of School/Senior Leader/IT Leader /Class teacher
- monitoring software/systems are implemented and updated as agreed in MAT/school policies

Teaching and Support Staff: Are responsible for ensuring that:

- they have an up to date awareness of on-line safety matters and of the current MAT/school On-line Safety Policy and practices
- they have read, understood and signed the MAT/school Staff Acceptable Use Policy/Agreement (AUP)
- they report any suspected misuse or problem to the on-line safety/IT Leader for investigation/ action/sanction
- digital communications with pupils (email/voice) should be on a professional level and only carried out using official MAT/school systems
- on-line issues are embedded in all aspects of the curriculum and other school activities
- pupils understand and follow the MAT/school On-line 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 IT activity in lessons, extra-curricular and extended school activities
- they are aware of on-line safety issues related to the use of mobile phones, cameras and hand-held devices and that they monitor their use and implement current MAT/school policies with regard to these devices
- in lessons where internet use is pre-planned 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

DSL/MAT Child Protection Officer: Should be trained in on-line 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

Parents/Carers: Play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of IT than their children.

The MAT/school will therefore take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, text, website and information about national / local on-line safety campaigns / literature. Parents and carers will be responsible for;

- endorsing (by signature) the Pupil Acceptable Use Policy
- accessing the school website/on-line pupil records in accordance with the relevant school Acceptable Use Policy (AUP).
- 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 of pupils in on-line safety is therefore an essential part of the MAT/school's on-line safety provision. Children and young people need the help and support of the school to recognise and avoid on-line safety risks and build their resilience. On-line education will be provided in the following ways;

- planned on-line safety programme should be provided as part of Computing/SMSC/other lessons and should be regularly revisited – this will cover both the use of IT and new /emerging technologies in school and outside school
- key on-line safety messages should be reinforced as part of a planned programme of assemblies and tutorial/pastoral activities
- 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
- pupils should be helped to understand the need for the pupil AUP and encouraged to adopt safe and responsible use of IT, the internet and mobile devices both within and outside school
- pupil should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet

Rules for use of IT systems/internet: Will be posted in all rooms and displayed on log-on screens. Staff should act as good role models in their use of IT, the internet and mobile devices.

Parents/Carers: Many parents and carers have only a limited understanding of on-line 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. "There is a generational digital divide". (Byron Report).

The MAT/school will therefore seek to provide information and awareness to parents and carers through;

- letters, newsletters, web site, text
- parents evenings
- signposting to safeguarding and internet safety websites

Staff Training: It is essential that all MAT and school staff receive on-line safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- planned programme of formal on-line safety training will be made available to staff. An audit of the on-line safety training needs of all school staff will be carried out regularly by individual school leaders.
- new staff should receive on-line safety training as part of their induction programme, ensuring that they fully understand the school On-line Safety Policy and Acceptable Use Policies
- On-line Safety/IT Leader will receive regular updates through attendance at external training sessions and by reviewing guidance documents released by SWGfl/LA and others
- this On-line Safety Policy and its updates will be presented to and discussed by staff in staff/team meetings/INSET days
- the On-line Safety/IT Leader will provide advice/guidance/training as required to individuals

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

- attendance at training provided by the MAT/ Local Authority/National Governors Association or another relevant organisation
- participation in school training/information sessions for staff or parents

Technical – Infrastructure/Equipment, Filtering and Monitoring: MAT/School will be responsible for ensuring that the IT 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 on-line safety responsibilities;

- IT systems will be managed in ways that ensure that the MAT/school meets the on-line safety technical requirements outlined in the MAT Security Policy and Acceptable Usage Policy and any relevant On-line Safety Policy and guidance
- there will be regular reviews and audits of the safety and security of MAT/school IT systems with the MAT IT Service provider
- servers, wireless systems and cabling must be securely located and physical access restricted
- all users will have clearly defined access rights to MAT/school IT systems. Details of the access rights available to groups of users will be recorded by the Network Manager (or other person) and will be reviewed, at least annually, by the on-line safety leader

- all users (at KS2 and above) will be provided with a username and password by the school IT technician who will keep an up to date record of users and their usernames. Use by pupils in this way should always be supervised and members of staff should never use a class log on for their own network access.
- schools should also consider the implications of the development of Learning Platforms and home access on whole class log-ons and passwords
- "administrator" passwords for the school IT system, used by the Network Manager (or other person) must also be available to the Head Teacher/Head of School or other nominated senior leader and kept in a secure place (e.g. school safe)
- alternatively, where the system allows more than one "administrator" log-on, the Head Teacher/Head of School or other nominated senior leader should be allocated those master/administrator rights
- users will be made responsible for the security of their username and password and 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.
- school maintains and supports the managed filtering service provided by our IT Service Providers 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/Head of School (or other nominated senior leader)
- filtering issues should be reported immediately to our filtering service providers
- requests from staff for sites to be removed from the filtered list will be considered by the Network Manager and IT. If the request is agreed, this action will be recorded, and logs of such actions shall be reviewed regularly by the on-line safety leader
- IT technical staff regularly monitor and record the activity of users on the MAT/school IT systems and users are made aware of this in the Acceptable Use Policy
- an appropriate system is in place (to be described) for users to report any actual / potential on-line incident to the Network Manager (or other relevant person)
- 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 MAT/school systems and data
- agreed policy is in place (to be described) for the provision of temporary access of "guests" (e.g. trainee teachers, visitors) onto the school system.
- agreed policy is in place regarding the downloading of executable files by users
- agreed policy is in place (to be described) regarding the extent of personal use that users (staff/pupils/community users) and their family members are allowed on laptops and other portable devices that may be used out of school
- agreed policy is in place that allows forbids staff from installing programmes on school workstations/portable devices
- agreed policy is in place (to be described) regarding the use of removable media (e.g. memory sticks/CDs/DVDs) by users on school workstations/portable devices
- MAT/school infrastructure and individual workstations are protected by up to date virus software. Personal data must not be sent over the internet or taken off the school site unless safely encrypted or otherwise secured (see GDPR policy)

Curriculum: On-line safety should be a focus in all areas of the curriculum and staff should reinforce on-line safety messages in the use of IT across the curriculum;

- in lessons where internet use is pre-planned, it is best practice that 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 pupils are allowed to freely search the internet, e.g. 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 (e.g. racism, drugs, and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Network Manager and IT Technician 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
- 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
- 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, MAT/school 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;

- when using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites
- staff are allowed to take digital/video images to support educational aims but must follow MAT/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 e.g. mobile phones**
- care should be taken when taking digital/video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the MAT/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 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

Data Protection

This policy meets the requirement of the Data Protection Act 1998 and is based on our GDPR policy which is based on guidance published by the Information Commissioner's Office and model privacy notices published by the Department of Education.

It also considers the provisions of the General Data Protection Regulations (GDPR), which came into force on 25 May 2018.

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 – **any loss of data or safety breach must be reported immediately to senior school leaders and the MAT GDPR Officer at Central Office**
- 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
  - ✓ the device must offer approved virus and malware checking software
  - ✓ the data must be securely deleted from the device, in line with school policy once it has been transferred or its use is complete

Communications

A wide range of rapidly developing/emerging communications technologies has the potential to enhance learning. The following table shows how the MAT/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	✓						✓	
Use of mobile phones in lessons				✓				✓

Use of mobile phones in social time (but not around pupils)	✓							✓
Taking photos on mobile phones or other camera devices				✓				✓
Use of hand-held devices e.g. tablets	✓						✓	
Use of personal email addresses in school, or on school network				✓				✓
Use of school email for personal emails				✓				✓
Use of chat rooms/facilities				✓				✓
Use of instant messaging				✓				✓
Use of social networking sites				✓				✓
Use of blogs	✓				✓			

When using communication technologies, the MAT/school considers the following as good practice;

- 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 (e.g. 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 MAT 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 – report directly to the MAT Operations officer at HR@andaras.org
- any digital communication between staff and pupils or parents / carers (email, chat, VLE etc.) must be professional in tone and content
- whole class or group email addresses will be used at KS1, while pupils at KS2 and above will be provided with individual school email addresses for educational use
- 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/on-line activity e.g. accessing child abuse images or distributing racist material is illegal and is obviously be banned from school and all other IT systems. Any concerns around these aspects must be reported to the MAT Operations Officer/Senior school Leader as soon as identified. Other activities e.g. cyber-bullying would be banned and could also 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 those users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The school 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					✓
	promotion or conduct of illegal acts, e.g. under the child protection, obscenity, computer misuse and fraud legislation					✓
	adult material that potentially breaches the Obscene Publications Act in the UK					✓
	criminally racist material in UK					✓
	pornography				✓	
	promotion of any kind of discrimination				✓	
	promotion of racial or religious hatred				✓	
	threatening behaviour, including promotion of physical violence or mental harm				✓	
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				✓	
Using school systems to run a private business					✓	
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by MAT and/or the school					✓	
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions					✓	✓
Revealing or publicising confidential or proprietary information (e.g. financial/ personal information, databases, computer / network access codes and passwords)					✓	
Creating or propagating computer viruses or other harmful files					✓	✓

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)		✓			
On-line gaming (non-educational)				✓	
On-line gambling				✓	
On-line shopping /commerce				✓	
File sharing				✓	
Use of social networking sites				✓	
Use of video broadcasting e.g. You-tube		✓	✓		

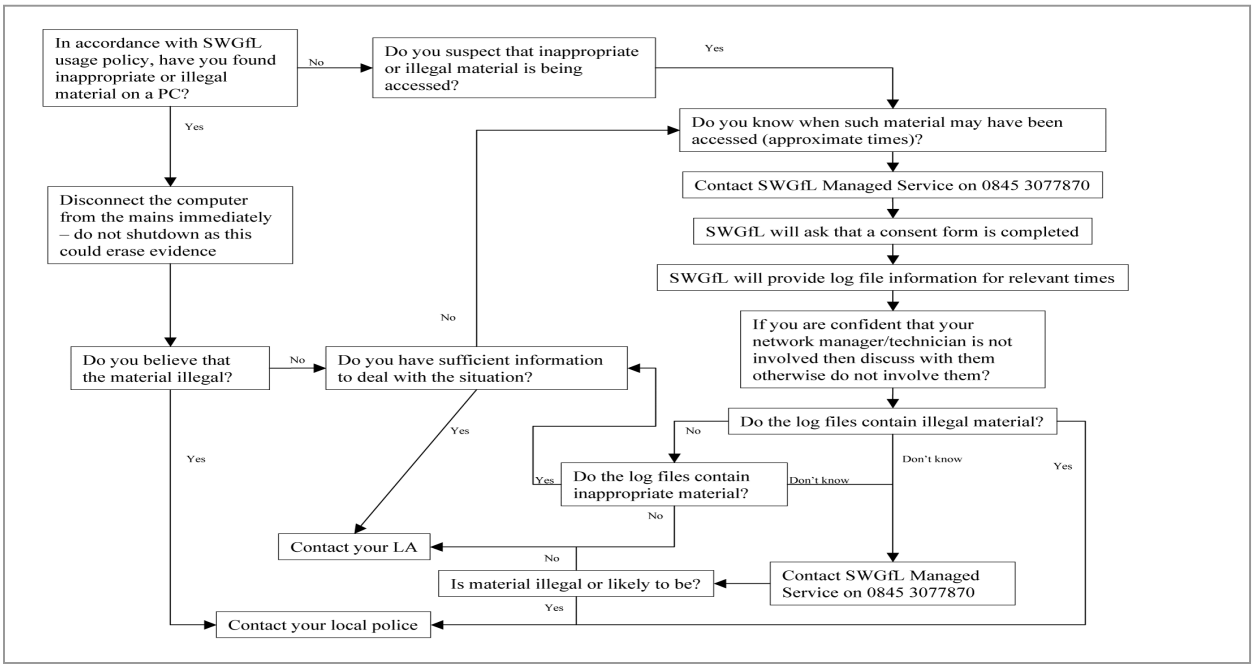
Responding to Incidents of Misuse

It is hoped that all members of the MAT/school community will be responsible users of IT, who understand and follow this On-line Safety 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 i.e.

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

the SWGfl flow chart – below and http://www.SWGfl.org.uk/safety/default.asp should be consulted and actions followed in line with the flow chart, in particular the sections on reporting the incident to the police and the preservation of evidence



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. In such event the MAT/school follows the SWGfl "Procedure for Reviewing Internet Sites for Suspected Harassment and Distress". This can be found on the SWGfl Safe website within the "Safety and Security booklet".
This guidance recommends that more than one member of MAT/school staff is involved in the investigation which should be carried out on a "clean" designated computer.
It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the 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 as follows

Pupils Actions / Sanctions

Incidents:	Refer to class teacher	Refer to Head of Department / other	Refer to Head of School	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 e.g. detention / exclusion
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 school network by					✓				

sharing username and passwords									
Attempting to access or accessing the school network, using another pupil's account	✓								
Attempting to access or accessing the school 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 school into disrepute or breach the integrity of the ethos of the school			✓						
Using proxy sites or other means to subvert the school'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	✓								

Staff	Actions / Sanctions

Incidents:	Refer to line manager	Refer to Head of School	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).		✓	✓	✓				
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 school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	✓	✓						
Careless use of personal data e.g. 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/pupils		✓						
Actions which could compromise the staff member's professional standing		✓						
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		✓						
Using proxy sites or other means to subvert		✓						

the school'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								