St Michael's Academy

St. Michael's Academy Policy for **E Safety**	**Date signed off:** Jan 18	No.
		Pg. /
	Review Date: Summer Term 2020	

This policy sets out the ways in which the Academy will:

- educate all members of the Academy community on their rights and responsibilities with the use of technology;
- build both an infrastructure and culture of e-Safety;
- work to empower the Academy community to use the Internet as an essential tool for life-long learning.

This policy is used in conjunction with other Academy policies.

This policy has been developed by a working group which included representatives from all groups within the Academy.

Scope of policy

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

The Education and Inspections Act 2006 empowers Principals, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the Academy site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents such as cyber-bullying, which may take place out of the Academy, but are linked to membership of the Academy.

The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

Signed by Chair……………………………………………………..Date……………………

The Academy will manage e-Safety as described within this policy and associated behaviour and anti-bullying policies, and will inform parents and carers of known incidents of inappropriate e-Safety behaviour that take place in and out of Academy.

Schedule for Development, Monitoring and Review

The Implementation of the e-Safety policy will be monitored by the SLT, meeting termly and reporting to the Governors annually.

The impact of the policy will be monitored by the deputy head teacher by looking at:

- Log of reported incidents
- Internet monitoring log
- Surveys or questionnaires of learners, staff, parents and carers
- Other documents and resources
- Future developments

The e-Safety policy will be reviewed annually or more regularly in the light of significant new developments in the use of technologies, new threats to e-Safety or incidents that have taken place.

The e-Safety policy approved by Governing body on ____________________________________

Signature of Chair of Governors: ____________________________________

The next review date is: ____________________________________

Signed by Chair………………………………………………………..Date……………………

Roles and responsibilities

The Headteacher is responsible for ensuring the safety (including e-Safety) of all members of the Academy community, though the day to day responsibility for e-Safety can be delegated.

The deputy head teacher will have overview of the serious child protection issues to arise from sharing of personal data, access to illegal or inappropriate materials, inappropriate on-line contact with adults, potential or actual incidents of grooming and cyber-bullying.

An e-Safety working group will work with the e-Safety Leader to implement and monitor the e-Safety policy and AUPs (Acceptable User Policies). This group is made up of the deputy head teacher, computing lead, governor with responsibility for safeguarding, IT technician and pupils. Pupils are part of this group, working with them through the Academy council, to contribute their knowledge and use of technology. They meet on a termly basis.

Role	**Responsibility**
Governors	• Approve and review the effectiveness of the e-Safety Policy • Delegate a governor to act as e-Safety link • e-Safety Governor works with the e-Safety Leader to carry out regular monitoring and report to Governors
Headteacher	• Ensure that all staff receive suitable CPD to carry out their e-Safety roles • Create a culture where staff and learners feel able to report incidents • Ensure that there is a system in place for monitoring e-Safety • Follow correct procedure in the event of a serious e-Safety allegation being made against a member of staff or pupil • Inform the local authority about any serious e-Safety issues • Ensure that the Academy infrastructure/network is as safe and secure as possible • Ensure that policies and procedures approved within this policy are implemented • Use an audit[1] to annually review e-Safety with the Academy's technical support
e-Safety Leader (Deputy Head Teacher)	• Lead the e-Safety working group • Log, manage and inform others of e-Safety incidents • Lead the establishment and review of e-Safety policies and documents • Ensure all staff are aware of the procedures outlined in policies relating to e-Safety • Provide and/or broker training and advice for staff • Attend updates and liaise with the LA e-Safety staff and technical staff • Meet with Senior Leadership Team and e-Safety Governor to regularly discuss incidents and developments • Coordinate work with the Academy's designated Child Protection Coordinator

[1] http://bit.ly/tech_esafety_check – Document from eLIM indicating questions SLT could ask

Signed by Chair…………………………………………………..Date……………………

Teaching and Support Staff	• Participate in any training and awareness raising sessions • Read, understand and sign the Staff AUP • Act in accordance with the AUP and e-Safety Policy • Report any suspected misuse or problems to the e-Safety Leader • Monitor ICT activity in lessons, extracurricular and extended Academy activities • Provide appropriate e-safety learning opportunities as part of a progressive e-safety curriculum and respond • Model the safe use of technology • Demonstrate consistently high standards of personal and professional conduct especially in relation to use of social networks, making sure that these are in line with Academy ethos and policies, including at the time of a Critical Incident
Pupils	• Read, understand and agree class internet rules • Participate in e-Safety activities, follow the AUP and report any suspected misuse • Understand that the e-Safety Policy covers actions out of Academy that are related to their membership of the Academy
Parents and Carers	• Endorse (by signature) the Home School Agreement • Discuss e-Safety issues with their child(ren) and monitor their home use of ICT systems (including mobile phones and games devices) and the internet • Access the Academy website in accordance with the relevant Academy AUP • Keep up to date with issues through newsletters and other opportunities • Inform the Principals of any e-Safety issues that relate to the Academy • Maintain responsible standards when using social media to discuss Academy issues
Technical Support Provider	• Ensure the Academy's ICT infrastructure is as secure as possible • Ensure users may only access the Academy network through an enforced password protection policy for those who access children's data • Maintain and inform the Senior Leadership Team of issues relating to filtering • Keep up to date with e-Safety technical information and update others as relevant • Ensure use of the network is regularly monitored in order that any misuse can be reported to the e-Safety Leader for investigation

Signed by Chair…………………………………………………..Date……………………

	• Ensure monitoring systems are implemented and updated • Ensure all security updates are applied (including anti-virus and Windows) • Sign an extension to the Staff AUP detailing their extra responsibilities[2]
Community Users	• Sign and follow the Guest/Staff AUP before being provided with access to Academy systems • Use the Online Compass tool[3] to review e-Safety

Education of pupils

Pupils to 'understand what constitutes unsafe situations and are highly aware of how to keep themselves and others safe in different situations including in relation to e-safety'

Academy Inspection Handbook - Ofsted 2018

A progressive planned e-Safety education programme takes place through discrete lessons and across the curriculum, for all children in all years, and is regularly revisited.

Breadth and progression is ensured through implementation of the Somerset ActiveBYTES 2017 and the e-safety progression that is part of the Somerset Primary Computing Curriculum/Somerset Byte Guide to SWGfL Digital Literacy Materials for KS3 and 4.

- Key e-Safety messages are reinforced through assemblies and Safer Internet Week (February) and throughout all lessons.
- Pupils are taught to keep themselves safe online and to be responsible in their use of different technologies as detailed in the Wessex planning.
- Pupils are guided to use age appropriate search engines for research activities. Staff are vigilant in monitoring the content of the websites visited and encourage pupils to use specific search terms to reduce the likelihood of coming across unsuitable material.
- In lessons where internet use is pre-planned, pupils are guided to sites checked as suitable for their use and processes are in place for dealing with any unsuitable material that is found in internet searches. Staff pre-check any searches.
- Pupils are taught to be critically aware of the content they access on-line and are guided to validate the accuracy and reliability of information.
- Pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Pupils are taught about current issues such as online gaming, extremism, blogging and obsessive use of technology
- Pupils will read, understand and agree for their class [*which might be agreed class rules*] at the beginning of each Academy year, which will be shared with parents and carers.

- Pupils are educated to recognise and respond appropriately to ‘different forms of bullying, including cyber-bullying’

Education and information for parents and carers

Parents and carers will be informed about the ways the internet and technology is used in Academy. They have a critical role to play in supporting their children with managing e-Safety risks at home, reinforcing key messages about e-Safety and regulating their home experiences. The Academy supports parents and carers to do this by:

- Providing clear guidance in the home school agreement which they are asked to sign with their children, regular newsletters and web site updates;

Comment [EW1]: Do we have an Acceptable Use Policy? I don’t think I have ever signed one!

- Raising awareness through activities planned by pupils;
- Inviting parents to attend workshops relating to E-Safety.
- providing and maintaining links to up to date information on the Academy website

Education of wider Academy community

The Academy provides information about e-Safety to organisations using Academy facilities and local play groups and nurseries. Details about the Online Compass review tool will be shared with these groups and members of the wider community which where appropriate include:

- details about the Online Compass review tool
- e-safety messages targeted to grandparents and other relatives

Training of Staff and Governors

There is a planned programme of e-Safety training for all staff and governors to ensure they understand their responsibilities, as outlined in this. This includes:

- An annual audit of the e-Safety training needs of **all** staff.
- **All** new staff receiving e-Safety training as part of their induction programme.

- providing information to supply and student teachers on the Academy’s e-safety procedures
- The e-Safety Leader receiving regular updates through attendance at SWGfL and LA training sessions and by reviewing regular e-Safety newsletters from the LA.
- This e-Safety Policy and its updates being shared and discussed in staff meetings.
- The e-Safety Leader providing guidance and training as required to individuals and seeking LA support on issues.

Signed by Chair…………………………………………………..Date……………………

Staff and governors are made aware of https://www.saferinternet.org.uk/professionals-online-safety-helpline 0344 3814772

-

Cyberbullying

Cyberbullying (along with all other forms of bullying) of any member of the Academy community will not be tolerated. Full details are set out in the Academy's policy on anti-bullying and behaviour.

- The Academy will follow procedures in place to support anyone in the Academy community affected by cyberbullying.
- Pupils and staff are made aware of a range of ways of reporting concerns about cyberbullying e.g. telling a trusted adult, Online bully box, Childline Phone number 0800 1111.
- Pupils, staff and parents and carers will be encouraged to report any incidents of cyberbullying and advised to keep electronic evidence.
- All incidents of cyberbullying reported to the Academy will be recorded.
- The Academy will follow procedures to investigate incidents or allegations of cyberbullying.
- Pupils, staff and parents and carers will be advised to keep a record of the bullying as evidence.
- The Academy will take steps where possible and appropriate, to identify the bully. This may include examining Academy system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police.
- Pupils, staff and parents and carers will be required to work with the Academy to support the approach to cyberbullying and the Academy's e-Safety ethos.
- Sanctions for those involved in cyberbullying will follow those for other bullying incidents and may include:
  - The bully will be asked to remove any material deemed to be inappropriate or a service provider may be contacted to remove content if the bully refuses or is unable to delete content.
  - Internet access may be suspended at the Academy for a period of time. Other sanctions for pupils and staff may also be used in accordance to the Academys anti-bullying, behaviour policy or AUP.
  - Parent and carers of pupils will be informed.
  - The police will be contacted if a criminal offence is suspected.

Technical Infrastructure

The Academy ensures, when working with our technical support provider that the following guidelines are adhered to:

- The Academy ICT systems are managed in ways that ensure that the Academy meets e-Safety technical requirements

- There are regular reviews and audits of the safety and security of Academy ICT systems[4].

- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations etc from accidental or malicious attempts which might threaten the security of the Academy systems and data with regard to:

  - the downloading of executable files by users

  - the extent of personal use that users (staff/pupils/community users) and their family members are allowed on laptops and other portable devices used out of Academy

  - the installing programs on Academy devices unless permission is given by the technical support provider or ICT coordinator

  - the use of removable media (e.g. memory sticks) by users on Academy devices. Should not be used. Ideally, all users should be aware that using OneDrive (it comes with your email system) is the best method for storing files as it's encrypted and on Microsoft's servers.

  - the installation of up to date virus software

- Access to the Academy network and internet will be controlled with regard to:

  - users having clearly defined access rights to Academy ICT systems through group policies

  - users (apart from Foundation Stage and Key Stage One pupils) being provided with a username and password

  - users being made aware that they are responsible for the security of their username and password and must not allow other users to access the systems using their log on details

  - users must immediately report any suspicion or evidence that there has been a breach of security

  - an agreed process being in place for the provision of temporary access of "guests" (e.g. trainee teachers, visitors) onto the Academy system. All "guests" must sign the staff AUP and are made aware of this e-Safety policy

  - Key Stage 2 pupil's will be supervised. Pupils will use age-appropriate search engines and online tools and activities which will be adult directed

- The internet feed will be controlled with regard to

  - the Academy maintaining a managed filtering service provided by an educational provider

[4] http://bit.ly/tech_esafety_check

- the Academy monitoring internet use
- requests for blocking sites for pupils has been logged via an email to the school IT technician in the past and then passed on to the Internet provider.
- any filtering issues being reported immediately to the IDN helpline.

- The ICT System of the Academy will be monitored with regard to:
- the Academy ICT technical support regularly monitoring and recording the activity of users on the Academy ICT systems
- e-Safety incidents being documented and reported immediately to the e-Safety Leader who will arrange for these to be dealt with immediately in accordance with the AUP

Data Protection

The SWGfL Data Protection Policy[5] provides full details of the requirements that need to be met in relation to the Data Protection Act 1998.

The Academy will:

- 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
- ensure that users are properly "logged-off" at the end of any session in which they are accessing personal data
- store or transfer data using Somerset Learning Platform (SLP), encryption and secure password protected devices
- make sure data is deleted from the device or SLP once it has been transferred or its use is complete

Use of digital and video images

Photographs and video taken within Academy are used to support learning experiences across the curriculum, to share learning with parents and carers on our Academy's learning platform and to provide information about the Academy on the website. The Academy will:

- When using digital images, instruct staff to educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images including on social networking sites.

[5] http://bit.ly/elimsomersetpolicies

Signed by Chair…………………………………………………..Date……………………

- Allow staff to take images to support educational aims, but follow guidance in the acceptable use policy concerning the sharing, distribution and publication of those images.

- Make sure that images or videos that include pupils will be selected carefully and will not provide material that could be reused.

- seek permission from parents or carers before images or videos of pupils are electronically published

- Encourage pupils to seek permission from other pupils to take, use, share, publish or distribute images of them without their permission

- all parties must recognise that any published image could be reused and repurposed

- Make sure that pupils' full names will not be used anywhere on the Academy website, particularly in association with photographs.

- Written permission from parents or carers will be obtained before images or videos of pupils are electronically published.

- Not publish pupils' work without their permission and the permission of their parents.

- Keep the written consent where pupils' images are used for publicity purposes, until the image is no longer in use.

- Publish a policy[6] regarding the use of photographic images of children which outlines policies and procedures.

Communication (including use of Social Media)

A wide range of communications technologies have the potential to enhance learning. The Academy will:

- **with respect to email**

  - Ensure that all Academy business will use the official Academy email service.

  - Ensure that any digital communication between staff and pupils or parents and carers (email, chat, VLE etc) is professional in tone and content.

  - Make users aware that email communications may be monitored.

  - Inform users what to do if they receive an email that makes them feel uncomfortable, is offensive, threatening or bullying in nature.

  - Provide whole class or group email addresses for use at Key Stage 1.

  - Provide pupils at Key Stage 2 and above with individual Academy email addresses for educational use only.

  - Teach pupils about email safety issues through the scheme of work and implementation of the AUP.

[6] http://bit.ly/elimsomersetpolicies

  - Ensure that personal information is not sent via email.
  - Only publish official staff email addresses.

- **with respect to social media** e.g. YouTube, Facebook, Twitter, blogging and personal publishing

- enable online learning opportunities to make use of age appropriate educationally focussed sites that will be moderated by the Academy

- control access to social media and social networking sites in Academy

- have a process to support staff who wish to use social media in the classroom to safely set up and run a class blog/Twitter/YouTube account to share learning experiences

- provide staff with the tools to risk assess sites before use and check the sites terms and conditions to ensure a) the site is age appropriate b) whether content can be shared by the site or others without additional consent being given

- make sure that staff official blogs or wikis will be password protected and run from the Academy website with approval from the Senior Leadership Team

- ensure that any digital communication between staff and pupils or parents and carers is always professional in tone and content

- discuss with staff the personal use of email, social networking, social media and personal publishing sites as part of staff induction, building an understanding of safe and professional behaviour in line with Teaching Standards

- staff are advised that no reference should be made to pupils, parents/carers or Academy staff

- advise all members of the Academy community not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory

- register concerns (e.g. recording in e-safety log) regarding pupils' inappropriate use of email, social networking, social media and personal publishing sites (in or out of Academy) and raise with their parents and carers, particularly when concerning pupils' underage use of sites

- support staff to deal with the consequences of hurtful or defamatory posts about them online

- inform the staff that in the case of a **Critical Incident** they should not make any comment on social media without the permission of the senior management team

- Inform staff not to run social network spaces for pupil use on a personal basis.

- **with respect to personal publishing**

  - Teach pupils via age appropriate sites that are suitable for educational purposes. They will be moderated by the Academy where possible.

  - Advise all members of the Academy community not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.

  - Register concerns regarding pupils' use of email, social networking, social media and personal publishing sites (in or out of Academy) and raise with their parents and carers, particularly when concerning pupils' underage use of sites.

  - Discuss with staff the personal use of email, social networking, social media and personal publishing sites as part of staff induction.

  - Outline safe and professional behaviour.

- **with respect to mobile phones**

  - Allow staff to bring mobile phones into Academy but must only use them during break, lunchtimes or during non-contact when they are not in contact with pupils' unless they have the permission of the Headteacher. They are not allowed to take photographs or video in Academy for any purpose without the express permission of the Senior Leadership Team.

- inform all that personal devices should be password protected

  - Advise staff not to use their personal mobile phone to contact pupils, parents and carers.

  - Provide a mobile phone for activities that require them.

- inform visitors of the Academy's expectations regarding the use of mobile phones

  - Allow pupils to bring mobile phones into Academy but only for use at specified times and for approved activities.

- maintain the right to collect and examine any phone that is suspected of containing offensive, abusive or illegal content or is suspected of causing issues on the Academy Internet connection

- **with respect to other personal devices**

- encourage pupils to bring their own device to support planned learning experiences

- ensure pupils using their own device sign an addition to the pupil AUP to agree to responsible use

- The staff AUP will apply to staff using their own portable device for Academy purposes

- enable and insist on the use of the Academy's Internet connection while on the Academy site

- Inform all that personal devices should be charged prior to bringing it to Academy
- maintain the right to collect and examine any device that is suspected of containing offensive, abusive or illegal content or is suspected of causing issues on the Academy Internet connection

The following table shows how the Academy considers how all these methods of communication should be used.

	Staff & other adults				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 Academy								
Use of mobile phones in lessons								
Use of mobile phones in social time								
Taking photos on mobile phones or other camera devices								
Use of hand held devices e.g. PDAs								
Use of personal email addresses in Academy, or on Academy network								
Use of Academy email for personal emails								
Use of chat rooms / facilities								
Use of instant messaging								
Use of social networking sites								
Use of blogs								
Use of Twitter								
Use of YouTube								

Signed by Chair…………………………………………………………..Date……………………

Assessment of risk

Methods to identify, assess and minimise risks will be reviewed regularly. As technology advances the Academy will examine and adjust the e-Safety Policy. Part of this consideration will include a risk assessment:

- looking at the educational benefit of the technology
- considering whether the technology has access to inappropriate material.

However, due to the global and connected nature of internet content, it is not possible to guarantee that access to unsuitable material will never occur via a Academy computer. Neither the Academy nor Somerset County Council can accept liability for the material accessed, or any consequences resulting from internet use.

All users need to be reminded that the use of computer systems, without permission or for inappropriate purposes, could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to Police.

Reporting and Response to incidents

The Academy will follow Somerset's flowcharts[7] to respond to illegal and inappropriate incidents as listed in those publications. More than one member of staff (at least one should be a senior leader) will be involved in this process and the same designated computer will be used for the duration of any investigation. All sites and content checked will be recorded and screen shots, signed and dated, will be kept where this is appropriate. Should content being reviewed include images of Child abuse then the monitoring will be halted and referred to the Police immediately.

- All members of the Academy community will be informed about the procedure for reporting e-Safety concerns (such as breaches of filtering, cyberbullying, illegal content etc).
- The e-Safety Leader will record all reported incidents and actions taken in the Academy e-Safety incident log and in any other relevant areas e.g. Bullying or Child Protection log.
- The designated Child Protection Coordinator will be informed of any e-Safety incidents involving child protection concerns, which will then be escalated in accordance with Academy procedures.
- The Academy will manage e-Safety incidents in accordance with the Academy Behaviour Policy where appropriate.
- The Academy will inform parents and carers of any incidents or concerns in accordance with Academy procedures.
- After any investigations are completed, the Academy will debrief, identify lessons learnt and implement any changes required.
- Where there is cause for concern or fear that illegal activity has taken place or is taking place then the Academy will contact Somerset Children Safeguarding Team and escalate the concern to the police.

[7] http://bit.ly/somersetesafetyflowcharts

Signed by Chair……………………………………………………..Date……………………

- If the Academy is unsure how to proceed with any incidents of concern, then the incident may be escalated to the Safeguarding for Academys Adviser, Local Authority Designated Officer (LADO) or Senior ICT Adviser.

If an incident or concern needs to be passed beyond the Academy then the concern will be escalated to the Somerset Safeguarding Children's Board. Should serious e-Safety incidents take place, the following external persons and agencies should be informed:	**Jane Weatherill - Education Safeguarding Advisor** **Email:** JWeatherill@somerset.gov.uk **Tel:** 01823 355014 Local Authority Designated Officer (LADO) 0300 123 2224

The police will be informed where users 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, 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

Sanctions and Disciplinary proceedings

Sanctions and disciplinary procedures will be taken where users 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
- Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.
- pornography, adult or mature content
- promotion of any kind of discrimination, racial or religious hatred
- personal gambling or betting
- personal use of auction sites
- any site engaging in or encouraging illegal activity
- threatening behaviour, including promotion of physical violence or mental harm
- any other information which may be offensive to colleagues or breaches the integrity of the ethos of the Academy or brings the Academy into disrepute
- using Academy systems to run a private business

Signed by Chair…………………………………………………..Date……………………

- use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by SWGfL and the Academy
- 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 or personal information, databases, computer or network access codes and passwords)
- creating or propagating computer viruses or other harmful files
- carrying out sustained or instantaneous high volume network traffic (downloading or uploading files) that causes network congestion and hinders others in their use of the internet

In addition the following indicates Academy policy on these uses of the Internet:

	Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable
On-line gaming (educational)				
On-line gaming (non-educational)				
On-line gambling				
On-line shopping / commerce				
File sharing (using p2p networks)				

Sanctions for misuse: Pupils

The 2011 Education Act increased powers with regard to the searching for and of electronic devices and the deletion of data. These are applied through the Academy's Behaviour Policy.

Academys should populate the grid below marking appropriate possible sanctions.
Incidents will have unique contexts and may need different levels of sanctions especially in relation to their type and severity. Therefore ticks may appear in more than one column.
The ticks in place are actions which must be followed

Incidents:	Refer to class teacher / tutor	Refer to Head of Department / Head of Year / other	Refer to Principals	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 /				✓		✓			

Signed by Chair………………………………………………………..Date……………………

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

Sanctions/Actions Staff

Academys should populate the grid below marking appropriate possible sanctions.
Incidents will have unique contexts and may need different levels of sanctions especially in relation to their type and severity. Therefore marks may appear in more than one column
The marks in place are actions which must be followed.

Incidents:	Refer to line manager	Refer to Head teacher	Refer to Local Authority / HR	Refer to LADO(L)/Police(P)	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).				L,P				

Signed by Chair……………………………………………………..Date……………………

Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email								
Unauthorised downloading or uploading of files								
Allowing others to access Academy network by sharing username and passwords or attempting to access or accessing the Academy network, using another person's account								
Careless use of personal data 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 staff								
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature to learners				L				
Breech of the Academy e-safety policies in relation to communication with learners				L				
Using personal email / social networking / instant messaging / text messaging to carry out digital communications with pupils				L				
Actions which could compromise the staff member's professional standing								
Actions which could bring the Academy into disrepute or breach the integrity of the ethos of the Academy								
Using proxy sites or other means to subvert the Academy's filtering system								
Accidentally accessing offensive or pornographic material and failing to report the incident				L				
Deliberately accessing or trying to access offensive or pornographic material				L				
Breaching copyright or licensing regulations								
Continued infringements of the above, following previous warnings or sanctions								

Signed by Chair……………………………………………………..Date……………………