Viking Academy Trust

Online Safety Policy

The VIKING ACADEMY TRUST Online Safety Policy for all VAT schools, has been written after consultation with staff, SWGFL and following DfE guidance.

Approved by the Trust: Term 1 2016

Reviewed annually: Term 4

Last review date: Term 4 2018

Signed: Chair of Trust

Online Safety Policy

The Viking Academy Trust

Schools in the Viking Academy Trust (VAT)

These are:

Chilton Primary School
Ramsgate Arts Primary School
Upton Junior School

This 'Online Safety Policy' is for all the aforementioned schools.

Scope of the Policy

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

The Education and Inspections Act 2006 empowers Headteacher's to such extent as is reasonable, to regulate the behaviour of students when they are off the *Viking Academy Trust* site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other Online Safety incidents covered by this policy, which may take place outside of the *academy*, but is 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 (see appendix for template policy). In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

The *Viking Academy Trust* 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 Online Safety behaviour that take place out of school.

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

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned online safety curriculum should be provided as part of Computing / PHSE / other lessons and should be regularly revisited
- Key online safety messages should be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities
- Students should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Students should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.
- Students should be helped to understand the need for the "Student Acceptable Use Agreement" and encouraged to adopt safe and responsible use both within and outside academy.
- Staff should act as good role models in their use of digital technologies the internet and mobile devices
- In lessons where internet use is pre-planned, it is best practice that students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where students are allowed to freely search the internet, 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 Technical Staff (or other relevant designated 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.

1 Education – Parents / Carers

Many parents and carers have only a limited understanding of online 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 behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The Viking Academy Trust will therefore seek to provide information and awareness to parents and carers through:

- *Curriculum activities*
- *Letters, newsletters, web site, Learning Platform*
- *High profile events / campaigns e.g. Safer Internet Day*
- *swgfl.org.uk*
  www.saferinternet.org.uk/
  http://www.childnet.com/parents-and-carers

2 Education & Training – Staff / Volunteers

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy.

- A planned programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced.
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the Viking Academy Trust Online Safety Policy and Acceptable Use Agreements.
- *It is expected that some staff will identify online safety as a training need within the performance management process.*
- *The Online Safety Coordinator / Officer (or other nominated person) will receive regular updates through attendance at external training events (eg from SWGfL / LA / other relevant organisations) and by reviewing guidance documents released by relevant organisations.*
- *This Online Safety Policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.*

3 Technical – infrastructure / equipment, filtering and monitoring

The Viking Academy Trust will be responsible for ensuring that the Viking Academy Trust 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 online safety responsibilities:

- Viking Academy Trust technical systems will be managed in ways that ensure that the Viking Academy Trust meets recommended technical requirements
- There will be regular reviews and audits of the safety and security of Viking Academy Trust technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to Viking Academy Trust technical systems and devices.
- All users (Staff) will be provided with a username and secure password.
- Users are responsible for the security of their username.
- The "master / administrator" passwords for the Viking Academy Trust ICT system, used by the Network Manager (or other person) must also be available to the Executive *Headteacher / Head of School* and kept in a secure place (Chilton and Upton's safe)
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes.
- Internet filtering should ensure that children are safe from terrorist and extremist material when accessing the internet.
- *The Viking Academy Trust has provided enhanced / differentiated user-level*
- *Viking Academy Trust technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.*
- *An appropriate system is in place* (Esafety log) *for users to report any actual / potential technical incident / security breach to the relevant person, as agreed).*
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.

- An agreed policy is in place for the provision of temporary access of "guests" (eg trainee teachers, supply teachers, visitors) onto the school systems.
- *A "Staff acceptable use" policy is in place regarding the extent of personal use that users (staff / students / community users) and their family members are allowed on school devices that may be used out of school.*
- *An agreed policy is in place* – only network administrators can *install programmes on school devices.* (From Sept 2017 Chilton and Ramsgate Free School)

• *Staff can use removable media (eg memory sticks / CDs / DVDs) by users on school devices, However staff are actively encouraged to use Office 365 and One Drive. Please see "Staff Acceptable Use Policy."*

4 Mobile Technologies (including BYOD/BYOT)

- The school Acceptable Use Agreements for staff, pupils/students and parents/carers will give consideration to the use of mobile technologies
- The school allows:

	School Devices			Personal Devices		
	School owned for single user	School owned for multiple users	Authorised device	Student owned	Staff owned	Visitor owned
Allowed in school	*Yes*	*Yes*	*Yes*	*Yes*	*Yes*	*Yes*
Full network access	*Yes*	*Yes*	*Yes*	*No*	*No*	*No*
Internet only					*As a wifi guest*	*As a wifi guest*

4.1 Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and students need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry 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: (select / delete as appropriate)

- When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Written permission from parents or carers will be obtained before photographs of students are published on the school website / social media / local press
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at Viking Academy Trust events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other *students* in the digital / video images.
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school academy policies concerning the sharing, distribution and publication of those images. Those images should only be taken on Viking Academy Trust equipment, the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the Viking Academy Trust into disrepute.
- Students must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images.
- Students' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Student's work can only be published with the permission of the student and parents or carers.

4.2 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.

The Viking Academy Trust must ensure that:

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing".
- It has a Data Protection Policy (see appendix for template policy)
- It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)
- Responsible persons are appointed / identified - Senior Information Risk Officer (SIRO) and Information Asset Owners (IAOs)
- Risk assessments are carried out
- It has clear and understood arrangements for the security, storage and transfer of personal data
- Data subjects have rights of access and there are clear procedures for this to be obtained
- There are clear and understood policies and routines for the deletion and disposal of data
- There is a policy for reporting, logging, managing and recovering from information risk incidents
- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties

- There are clear policies about the use of cloud storage / cloud computing which ensure that such data transfer / storage meets the requirements laid down by the Information Commissioner's Office.
- 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, memory 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

4.3 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:

4.4 Communication Technologies

Personal Mobile phones may be brought to the academy, but not allowed to be used in lessons and not allowed to be used to take photographs

Staff must Use Viking Academy Trust email for professional reasons and not for personal emails. Staff can check personal email addresses, using the filtered internet access, at the correct time in school (breaktimes and before and after school.)

Use of social media and blogs are actively encouraged to promote the activities happening within schools and across the academy.

When using communication technologies the Viking Academy Trust considers the following as good practice:

- The official *Viking Academy Trust* email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. *Staff and students should therefore use only the Viking Academy Trust email service to communicate with others when in school, or on Viking Academy Trust systems (e.g. by remote access).*
- Users must immediately report, to the nominated person – in accordance with the Viking Academy Trust policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and students or parents / carers (email, social media, chat, blogs, VLE etc) must be professional in tone and content. *These communications may only take place on official (monitored) Viking Academy Trust systems. Personal email addresses, text messaging or social media must not be used for these communications.*
- *Students should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.*
- *Personal information should not be posted on the Viking Academy Trust website and only official email addresses should be used to identify members of staff.*

4.5 Social Media - Protecting Professional Identity

All schools, academies and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools/academies and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the *Viking Academy Trust* or local authority / academy group liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The Viking Academy Trust provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through:

- Ensuring that personal information is not published

- Training is provided including: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

Viking Academy Trust staff should ensure that:

- No reference should be made in social media to students / pupils, parents / carers or Viking Academy Trust staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the *school /academy* or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information

When official Viking Academy Trust social media accounts are established there should be:

- *A process for approval by senior leaders*
- *Clear processes for the administration and monitoring of these accounts – involving at least two members of staff*
- *A code of behaviour for users of the accounts, including*
- *Systems for reporting and dealing with abuse and misuse*
- *Understanding of how incidents may be dealt with under Viking Academy Trust disciplinary procedures*

Personal Use:

- Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with the Viking Academy Trust or impacts on the school/ academy, it must be made clear that the member of staff is not communicating on behalf of the Viking Academy Trust with an appropriate disclaimer. Such personal communications are within the scope of this policy
- Personal communications which do not refer to or impact upon the school are outside the scope of this policy
- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken

- *The Viking Academy Trust permits reasonable and appropriate access to private social media sites*

Monitoring of Public Social Media

- As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the school
- The school should effectively respond to social media comments made by others according to a defined policy or process

The *academy's* use of social media for professional purposes will be checked regularly by the senior risk officer and Online Safety Group to ensure compliance with the school policies.

4.6 Unsuitable / inappropriate activities

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

The Viking Academy Trust believes that the activities referred to in the following section would be inappropriate in a Viking Academy Trust context and that users, as defined below, should not engage in these activities in / or outside the Viking Academy Trust when using Viking Academy Trust equipment or systems. The Viking Academy Trust policy restricts usage as follows:

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated	Unacceptable	Unacceptable and illegal
Users shall not	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					X

	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	Pornography				X	
	Promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	Promotion of extremism or terrorism				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	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the academy					X	
Infringing copyright					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	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)					X	
On-line gaming (educational)		x				
On-line gaming (non-educational)			x			
On-line gambling					x	
On-line shopping / commerce			x			
File sharing (not Peer-2-Peer and torrenting) But sharing files.			x			

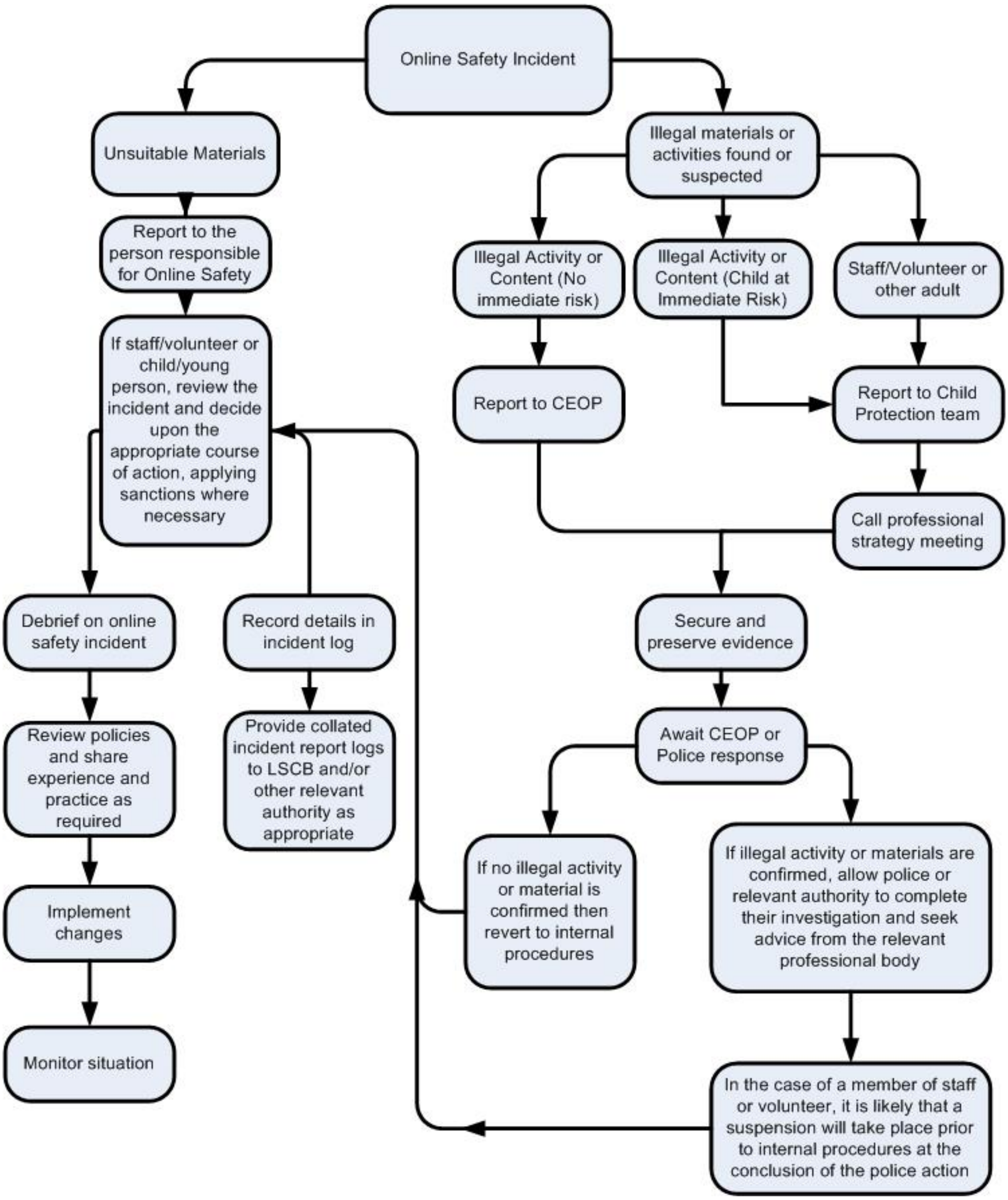
Use of social media		x			
Use of messaging apps		x			
Use of video broadcasting e.g. Youtube			x		

4.7 Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see "User Actions" above).

4.8 Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the police.


Online Safety Incident
Unsuitable Materials
Illegal materials or activities found or suspected
Report to the person responsible for Online Safety
Illegal Activity or Content (No immediate risk)
Illegal Activity or Content (Child at Immediate Risk)
Staff/Volunteer or other adult
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Report to CEOP
Report to Child Protection team
Call professional strategy meeting
Debrief on online safety incident
Record details in incident log
Secure and preserve evidence
Review policies and share experience and practice as required
Provide collated incident report logs to LSCB and/or other relevant authority as appropriate
Await CEOP or Police response
If no illegal activity or material is confirmed then revert to internal procedures
If illegal activity or materials are confirmed, allow police or relevant authority to complete their investigation and seek advice from the relevant professional body
Implement changes
Monitor situation
In the case of a member of staff or volunteer, it is likely that a suspension will take place prior to internal procedures at the conclusion of the police action

4.9 Other Incidents

It is hoped that all members of the Viking Academy Trust community will be responsible users of digital technologies, who understand and follow Viking Academy Trust policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff / volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
    - Internal response or discipline procedures
    - Involvement by Local Authority / Academy Group or national / local organisation (as relevant).
    - Police involvement and/or action

- If content being reviewed includes images of Child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:
    - incidents of 'grooming' behaviour
    - the sending of obscene materials to a child
    - adult material which potentially breaches the Obscene Publications Act
    - criminally racist material
    - promotion of terrorism or extremism

  - other criminal conduct, activity or materials
- Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for the *Viking Academy Trust* and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

4.10 Viking Academy Trust Actions & Sanctions

It is more likely that the Viking Academy Trust 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:

4.10.1	Actions / Sanctions								
Students Incidents	Refer to class teacher	Refer to Head of Year / AHT	Refer to Headteacher / EHT	Refer to Police	Refer to technical support staff for action re filtering / security etc.	Inform parents / carers	Removal of network / internet access	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	X	x	x	x	x	x
Unauthorised use of non-educational sites during lessons	x	x	x						
Unauthorised / inappropriate use of mobile phone / digital camera / other mobile device	x		x	x	x	x		x	x
Unauthorised / inappropriate use of social media / messaging apps / personal email	x	x	x						
Unauthorised downloading or uploading of files			x	x	x	X			
Allowing others to access Viking Academy Trust network by sharing username and passwords			x		X				
Attempting to access or accessing the Viking Academy Trust network, using another student's / pupil's account	x	x	x						
Attempting to access or accessing the Viking Academy Trust network, using the account of a member of staff		x	x	x	X				
Corrupting or destroying the data of other users	x	X	x	x	x	x	x		X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	x	x	x	x	x	x			

Continued infringements of the above, following previous warnings or sanctions							x		X
Actions which could bring the Viking Academy Trust into disrepute or breach the integrity of the ethos of the school		x	x						
Using proxy sites or other means to subvert the academy's filtering system		x	x	x	X				X
Accidentally accessing offensive or pornographic material and failing to report the incident			X		x	x			X
Deliberately accessing or trying to access offensive or pornographic material			x	x	x	X			X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act			x	x	x	x			

4.10.2

Actions / Sanctions

Staff Incidents	Refer to line managerr	Refer to Headteacher	Refer to Local Authority /	Refer to Police	Refer to Technical Support Staff for action re filtering	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		X		X
Inappropriate personal use of the internet / social media / personal email		x	x	x		X		x
Unauthorised downloading or uploading of files		x	x	x	X	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	X			
Careless use of personal data e.g. holding or transferring data in an insecure manner		x		x	X	X	X	x
Deliberate actions to breach data protection or network security rules		x		x	x	x	X	X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		x		x	x	x	X	X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		x	x		x	X	X	X
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils			x	x	x	x	X	X
Actions which could compromise the staff member's professional standing			x	x	x	X	X	X
Actions which could bring the Viking Academy Trust into disrepute or breach the integrity of the ethos of the Viking Academy Trust			x	x	x	x	X	X
Using proxy sites or other means to subvert the school's / academy's filtering system			x	X	x			
Accidentally accessing offensive or pornographic material and failing to report the incident			x	x	x	x	x	x

Deliberately accessing or trying to access offensive or pornographic material		x	x	x	x	x	x	X
Breaching copyright or licensing regulations		x	x	x	x	x	x	X
Continued infringements of the above, following previous warnings or sanctions		x	x	x	x	x	x	X