CECIL JONES

ACADEMY

E-Safety Policy

September 2018

Date created	March 2016
Version	1.1
Status	Published
Applicable to	Academy
Author	K.Henson
Checked by	SLT
Valid from	March 2016
Review on	September 2019

Contents Page:

A1 What is E-Safety?

A2 Risks within E-Safety

A3 Scope of policy

A4 Roles and responsibilities

A5 Education and curriculum

A6 Illegal or inappropriate activities or sanctions

A7 Reporting of E-Safety breaches

A8 Use of hand held technology

A9 Use of communication technologies

A10 Social Networking

A11 Video conferencing

A12 Use of digital and video images

A13 Use of website

A14 Professional standards for staff communication

Section B Infrastructure

B1 Password security

B2.1 Filtering

B2.1a Introduction

B2.1c Responsibilities

B2.1d Changes to the filtering system

B2.1e Monitoring

B2.1f Audit reporting

A1. What is E-Safety?

E- Safety is often defined as 'the safe and responsible use of technology' this includes:

- The use of the internet and other means of communication
- Using electronic devices (e.g. ipads/laptops/mobile phones/ cameras etc)
- Social media
- Gaming
- Email

In the context of an inspection, e- safety is described as the Academy's ability to:

- Protect and educate staff/students in their use of technology
- To have the appropriate mechanisms to intervene and support any incident where appropriate

A2. Risks within e-safety can be categorised as follows:

Content:

- Exposure to inappropriate content
- Content promoting harmful behaviours
- Hate content
- Content validation: how to check authenticity and accuracy of online content

Contact:

- Grooming (sexual exploitation, radicalisation, extremism)
- Online bullying in all forms

Conduct:

- Aggressive behaviours (bullying)
- Privacy issues, including disclosure of personal information
- Digital footprint and online reputation
- Health and wellbeing (amount of time spent online, gambling, body image)

A3. Scope of the policy:

This policy applies to all members of Cecil Jones community (staff, students, volunteers, parent/carers, visitors, community users) who have access to and are users of the Cecil Jones ICT systems both in and outside the academy.

The Education and Inspections ACT 2006 empowers head teachers, to such extent as is reasonable, to regulate the behaviour of students when they are off the Academy site and empowers members of staff to impose disciplinary sanctions for inappropriate behaviour. This is pertinent to incidents of cyberbullying or other e-safety incidents covered by this policy, which may take place out of the Academy, but are linked to the Academy. Please note this policy will need to read in conjunction with the Anti- bulling, child protection and safeguarding policy's.

The Academy will deal with incidents using guidance within this and will inform parents/carers of any e-safety incidents.

A4. Roles and responsibilities:

Role	Key Responsibilities
Governor responsible for e-safety	• Regularly meet with E-safety Co-ordinator/committee • Regular monitoring of E-safety incident logs • Regular monitoring of filtering/change control logs • Reporting to relevant Governors in meetings
Principal/SLT	• Has a duty of care for ensuring the safety (including e-safety of members of the Cecil Jones community. The day to day responsibility for e-safety will be delegated to the E-safety Co-ordinator and safeguarding lead. • The principle should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff • The principal is responsible for ensuring that the E-safety Co-ordinator and other relevant staff are e-safety trained to carry out their roles and train other colleagues. • Principal/Senior leaders will ensure that there is a system in place to allow for monitoring and support for all those who carry out the internal monitoring role. • SLT will receive regular monitoring reports from the E-Safety Co-ordinator • SLT to ensure that e-safety is taught and embedded in the curriculum
E-safety Coordinator:	• Leads the e-safety committee • Take the day to day responsibility for e-safety issues with the safeguarding lead • Has a leading role in establishing and reviewing the academy's e-safety policies/documents • Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place. • Receives reports of e-safety incidents from the safeguarding lead and create a log of incidents to inform future training. • Reports regularly to SLT
Network Manager/ Technical staff:	• Ensures that the academy's technical infrastructure is secure and is not open to misuse or malicious attack • Meets all the e-safety technical requirements and any Local Authority/other relevant body E-safety policy and guidance that might apply. • That users may only access the networks and devices through a properly enforced password protection policy In which passwords are regularly changed.
Teaching and Support Staff	• Have an updated awareness of e-safety matters and the current academy e-safety policy and practices

	• They have read and understood and signed the Staff Acceptable Use Policy (AUP agreement) • They report any misuse or problem to Safeguarding Lead e-safety Co-ordinator for investigation/action/sanction • All digital communications with students/parents/carers should be on a professional level and only carried out using the official Academy's systems • E- safety issues are embedded in all aspects of the curriculum and other activities • Students understand and follow the e-safety and acceptable use policies • Students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright Regulations They monitor the use of digital technologies, cameras, iPads etc. in lessons and other activities. • In lessons where internet is used, sites must be checked and suitable for the students use and inform technical staff if any unsuitable material appears.
Designated Safeguarding Lead	• To deal with any of the safeguarding issues that might arise from: • Sharing of personal data • Access to illegal/ inappropriate materials • Inappropriate on-line contact with adults/ strangers • Potential or actual incidents of grooming • Cyber-bullying
E- Safety committee	• Consultative group which has a wide representation from the academy • Monitoring and review the e-safety policy • Monitor and review the impact of e-safety in the curriculum
Students	• Are responsible for using the academy technology systems in accordance with the student Acceptable Use Policy • Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations. • Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so • To know what action to take if they or someone they knows feel vulnerable when using online technology. • To understand the importance of adopting safe behaviour and good online safety practice when using digital technologies outside of the academy.
Parents/Carers	• To read, understand and promote the Academy's the Student Acceptable Use Agreement with their child where appropriate • To consult the Academy if they have any concerns about their child's use of technology • Support the academy in promoting online safety and endorse the parent Acceptable Use Agreement which includes the students use of photographic and video images

Community Users:	- Any external individual/organisation will sign an Acceptable Use Agreement prior to using technology Or the internet within the Academy - To model safe, responsible and positive behaviours in their own use.

A5. Education and Curriculum

Student's online safety curriculum:

This academy:

- Is currently developing a clear progressive online safety education programme as part of the Computing curriculum / PSHE. This covers a range of skills and behaviours appropriate for their age, needs and experience.
- Key e-safety messages reinforced as part of a planned programme of assemblies and tutor programme
- Students taught in all lessons to be critically aware of the materials/content they access online
- Ensure staff model safe and responsible behaviour in their own use of technology e.g. use of passwords, logging off, use of content

Education – Parents/Carers

Many parents may have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring/regulation of their children's online 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.

Cecil Jones Academy will therefore seek to provide information and awareness to parents and carers through:

- Newsletter
- Letters
- Academy website
- High profile events e.g. Safer Internet Day
- Parent forum
- References for helpful websites / publications
- Request online parent training via the E-safety Co-ordinator

Education Staff/volunteers/ Governors training

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

- Training will be offered as follows:
- An e- safety audit will be carried out annually

- A planned programme of formal e-safety training will be made available to staff.
- All new staff should receive e-safety training as part of their induction programme and fully understand the Acceptable Use Agreements.

A6. Illegal or inappropriate activities and related sanctions:

Cecil Jones Academy believes that the activities below are inappropriate in an academy context **(Those in bold are illegal)** and users should not engage in these activities when using academy equipment or systems **(in or outside the academy).**

Users should not visit internet sites, make post, download, data transfer, communicate or pass on material, remarks, proposals or comments that certain or relate to:

- **Child sexual abuse images (illegal- The Protection of Children Act 1978)**
- **Grooming, incitement, arrangement or facilitation of sexual acts against children (illegal- Sexual Offences Act 2003)**
- **Possession of extreme pornographic images (illegal- Criminal Justice and immigration Act 2008)**
- **Criminally racist material in Uk- to stir up religious hatred (or hatred on the grounds of sexual orientation) (illegal –Public Order Act 1986)**
- Pornography
- Promotion of any kind of discrimination
- Promotion of radicalisation or extremism
- 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.

Additionally the following activities are also considered unacceptable on ICT equipment or infrastructure provided by the academy:

- Using the academy systems to undertake transactions pertaining to a private business
- Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed 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 / 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 gambling and non-educational gaming
- On-line shopping / commerce
- Use of social networking sites (other than in the academy's learning platform or sites otherwise permitted by the academy.

If members of staff suspect that misuse might have taken place – whether or not it is evidently illegal (see above) - it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation.

It is more likely that the academy 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 academy 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 indicated on the following pages.

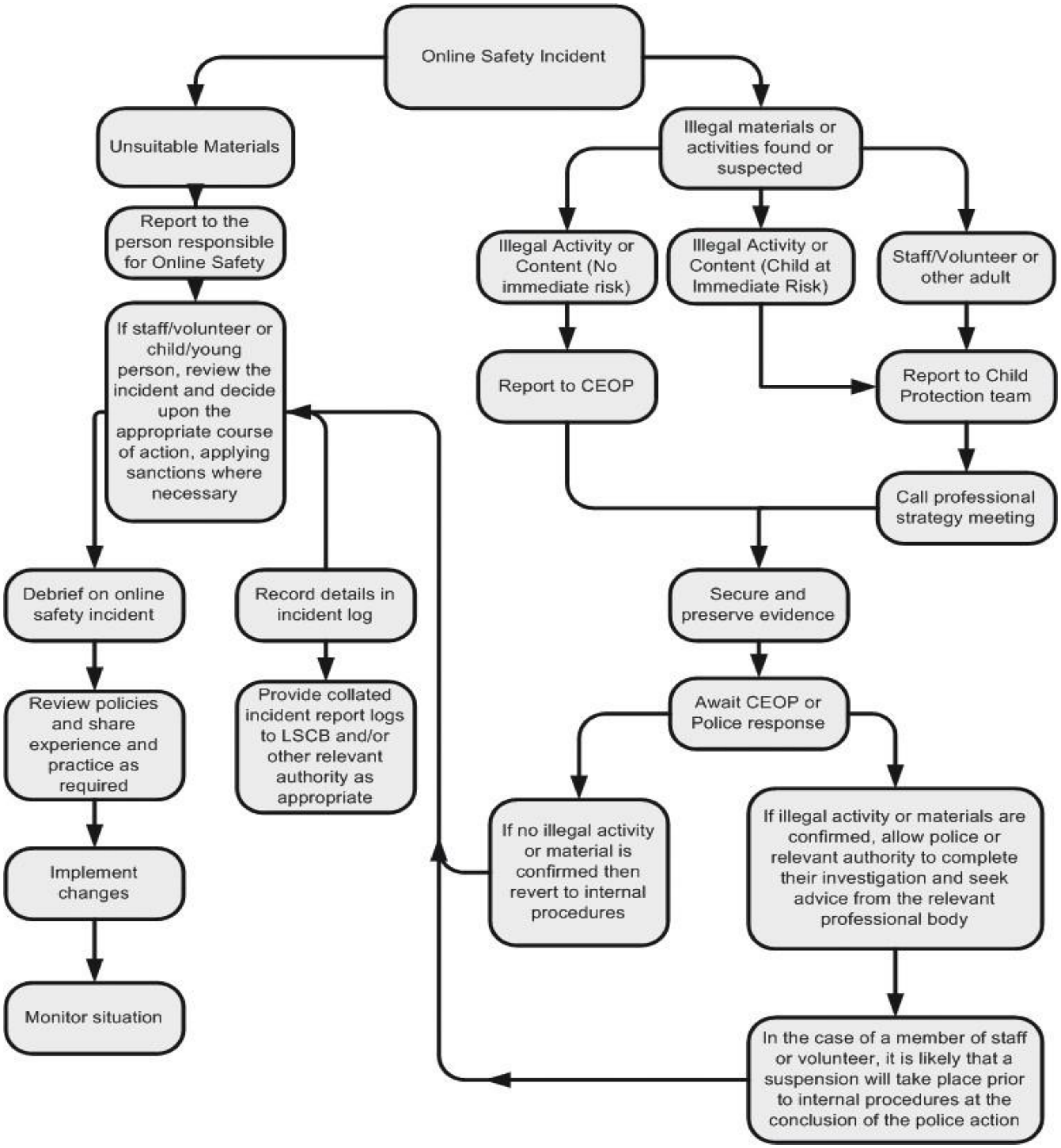
	Refer to:					Inform:	Action:		
Student sanctions	Class teacher	E-safety coordinator	Refer to Principal	Refer to Police	Refer to E-Safety Coordinator for action re filtering / security etc	Parents / carers	Removal of network / internet access rights	Warning/ sanction	Further sanction e.g. detention / 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 academy network by sharing username and passwords	/	/			/		/	/	
Attempting to access 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	/	/	/		/	/	/		/

	Refer to:					Action:		
Staff sanctions	Line manager	Principal /	safeguarding	Police	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 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	/	/			/	/		
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / students	/	/	/		/	/		
Actions which could compromise the staff member's professional standing	/	/						
Actions which could bring the academy into disrepute or breach the integrity of the ethos of the academy	/	/						
Using proxy sites or other means to subvert the academy's filtering system	/				/			
Accidentally accessing offensive or pornographic material and failing to report the incident	/	/	/		/	/		
Deliberately accessing or trying to access offensive or pornographic material	/	/	/	/	/	/	/	/
Breaching copyright or licensing regulations	/	/				/		
Continued infringements of the above, following previous warnings or sanctions	/	/			/			/

A7. Reporting of e-safety breaches

It is hoped that all members of the academy will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse:

Particular care should be taken if any apparent or actual misuse appears to involve illegal activity listed in section 6 of this policy


Online Safety Incident
Unsuitable Materials
Report to the person responsible for Online Safety
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Debrief on online safety incident
Review policies and share experience and practice as required
Implement changes
Monitor situation
Record details in incident log
Provide collated incident report logs to LSCB and/or other relevant authority as appropriate
Illegal materials or activities found or suspected
Illegal Activity or Content (No immediate risk)
Illegal Activity or Content (Child at Immediate Risk)
Staff/Volunteer or other adult
Report to CEOP
Report to Child Protection team
Call professional strategy meeting
Secure and preserve evidence
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
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

A8. Use of hand held technology (personal phones, tablets and other hand held devices)

We recognise that the area of mobile technology is rapidly advancing and it is our academy's policy to review its stance on such technology on a regular basis. Currently our policy is this:

- Members of staff are permitted to bring their personal mobile devices into academy. They are required to use their own professional judgement as to when it is appropriate to use them. Broadly speaking this is:
- Personal hand held devices will be used in lesson time only in an emergency or extreme circumstances
- Members of staff are free to use these devices outside teaching time.
- An academy mobile phone is available for all professional use (for example when engaging in off- site activities) and members of staff should not use their personal device for academy purposes except in an emergency.
- Students are permitted to bring their personal hand held devices into academy but not use them during lesson times unless directed by a member of staff.
- A number of such devices are available in academy (e.g. iPad, tablets) and are used by students as considered appropriate by members of staff.

	Staff / adults				Students			
Personal hand held technology	Allowed	Allowed at certain	Allowed for selected	Not allowed	Allowed	Allowed at certain	Allowed with staff	Not allowed
Mobile phones may be brought to the academy	/					/		
Use of mobile phones in lessons				/				/
Use of mobile phones in social time		/						/
Taking photos on personal phones or other camera devices				/				/
Use of hand held devices e.g. PDAs, gaming consoles	/						/	

A9. Use of communication technologies

- Email

- Access to email is provided for all users in the academy using their unique credentials.
- These official academy email services may be regarded as safe and secure and are monitored.
- Staff should use only the academy email services to communicate with others when in academy, or on academy systems (e.g. by remote access)
- Users need to be aware that email communications may be monitored
- A structured education programme is delivered to students which helps them to be aware of the dangers of and good practices associated with the use of email
- Staff should only access personal email accounts on academy systems for emergency or extraordinary purposes.
- Users must immediately report to their class teacher / E-Safety Coordinator, in accordance with the academy policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and they must not respond to any such email.

	Staff / adults				**Students**			
Use of Email	Allowed	Allowed at certain	Allowed for selected	Not allowed	Allowed	Allowed at certain	Allowed with staff	Not allowed
Use of personal email accounts in the academy / on the academy network				/				/
Use of academy email for personal use				/				/

A10. Social networking (including chat, instant messaging, blogging etc)

	Staff / adults				**Students**			
Use of social networking tools	Allowed	Allowed at certain	Allowed for selected	Not allowed	Allowed	Allowed at certain	Allowed with staff	Not allowed
Use of non educational chat rooms etc				/				/
Use of non educational instant messaging				/				/
Use of non educational social networking sites				/				/
Use of non educational blogs				/				/

A11- Videoconferencing

Desktop video conferencing and messaging systems linked to Skype is the preferred communication option in order to secure a quality of service that meets academy's curriculum standards.

- Videoconferencing equipment in classrooms are switched off when not in use and not set to auto answer.
- Only web based conferencing products that are authorised by the academy (and are not blocked by internet filtering) are permitted for classroom use.

- Videoconferencing is always supervised directly by a teacher.
- Only key administrators have access to videoconferencing administration areas.

A12. Use of digital and video images

- 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.
- Members of staff are allowed to take digital still and video images to support educational aims, but must follow academy policies concerning the sharing, distribution and publication of those images. Those images should only be captured using academy equipment; **the personal equipment of staff should not be used for such purposes.**
- Care should be taken when taking digital / video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the academy into disrepute.
- Students must not take, use, share, publish or distribute images of others without their permission See also the following section (A.3.4) for guidance on publication of photographs

A12. Use of web-based publication tools

Website (and other public facing communications)

Our academy uses the public facing website ceciljones.net only for sharing information with the community beyond our academy. This includes, from time-to-time, celebrating work and achievements of children. All users are required to consider good practice when publishing content.

- Personal information will not be posted on the academy website and only official email addresses will be used to identify members of staff (never students).
- Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with the following good practice guidance on the use of such images:
- students' full names will not be used anywhere on a website or blog, and never in association with photographs

- where possible, photographs will not allow individuals to be recognised
- written permission from parents or carers will be obtained before photographs of students are published on the academy website

A14. Professional standards for staff communication

In all aspects of their work in our academy, teachers abide by the broad **Professional Standards for Teachers** laid down by the TDA effective from September 2012:

Teachers translate these standards appropriately for all matters relating to e-safety.

Any digital communication between staff and students or parents / carers (email, chat, learning platform etc)
must be professional in tone and content.

- These communications may only take place on official (monitored) academy systems.
- Personal email addresses, text messaging or public chat / social networking technology must not be used for these communications.

Staff constantly monitor and evaluate developing technologies, balancing risks and benefits, and consider how appropriate these are for learning and teaching. These evaluations help inform policy and develop practice.

The views and experiences of students are used to inform this process also.

Section B. Infrastructure

B.1 Password security

The academy's e-safety curriculum will include frequent discussion of issues relating to password security and staying safe in and out of academy. Passwords will be periodically changed. Staff and students are not share their password.

B.2.1 Filtering

B.2.1a - Introduction

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so. It is therefore important that the academy has a filtering policy to manage the associated risks and to provide preventative measures which are relevant to the situation in this academy.

B.2.1b - Responsibilities

The day-to-day responsibility for the management of the academy's filtering policy is held by the systems manager (Phil Maddocks) with ultimate responsibility resting with the **Executive Principal and Governors**). They manage the academy filtering in line with this policy and keep logs of changes to and breaches of the filtering system.

To ensure that there is a system of checks and balances and to protect those responsible, changes to the standard filtering service must be reported to, and authorised by, a second responsible person prior to changes being made (this will normally be the class teacher who originally made the request for the change).

All users have a responsibility to report immediately to class teachers / E-Safety Coordinator any infringements of the academy's filtering policy of which they become aware or any sites that are accessed, which they believe should have been filtered.

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

B.2.1c - Education / training / awareness

Students are made aware of the importance of filtering systems through the academy's e-safety education programme.

Staff users will be made aware of the filtering systems through:

- signing the Acceptable Use Agreement (as part of their induction process)
- briefing in staff meetings, training days, memos etc. (timely and ongoing).

Parents will be informed of the academy's filtering policy through the Acceptable Use Agreement and through e- safety awareness sessions / newsletter etc

B.2.1d - Changes to the filtering system

Where a member of staff requires access to a website that is blocked for use at academy, the process to unblock is as follows:

- The teacher makes the request to the network manager
- The network manager checks the website content to ensure that it is appropriate for use in the academy.

THEN
The network manager unblocks the site and logs the action in the change-control log to be reported as described above

The network manager will need to apply a rigorous policy for approving / rejecting filtering requests. The site promotes equal and just representations of racial, gender, and religious issues.

- The site does not contain inappropriate content such as pornography, abuse, racial hatred and terrorism.

The site does not link to other sites which may be harmful / unsuitable for students.

B.2.1e - Monitoring

No filtering system can guarantee 100% protection against access to unsuitable sites. The academy will therefore monitor the activities of users on the academy network and on academy equipment.

Monitoring takes place as follows:

- Identified member(s) of staff reviews the monitoring console captures weekly
- "False positives" are identified and deleted
- Potential issues are referred to an appropriate person depending on the nature of the capture.
- Teachers are encouraged to identify in advance any word or phrase likely to be picked up regularly through innocent use (e.g. 'goddess' is captured frequently when a class is researching or creating presentations on the Egyptians) so that the word can be allowed for the period of the topic being taught.

B.2.1f - Audit / reporting

Filter change-control logs and incident logs are made available to:

- the e-safety governor within the timeframe stated in this policy
- the E-Safety Committee
- the LSCB on request

This filtering policy will be reviewed, with respect to the suitability of the current provision, in response to evidence provided by the audit logs.