ARTHUR MELLOWS VILLAGE COLLEGE

E-SAFETY POLICY

Presented to:

Governors' Students and Safeguarding Meeting
29 June 2021

Date approved:[1]	6 June 2017
Date reviewed:[2]	29 June 2021
Date of next review:[3]	Summer 2024

[1] This is the date the policy was approved by the meeting
[2] This is the date the policy was reviewed prior to its approval above
[3] This is the date as set by the policy review clause or the date approved plus two years

This policy must be read in conjunction with the Four Cs Trust General Data Protection Regulations Policy and the Trust's Staff ICT Policy.

1. SCOPE OF THE POLICY

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

1.1 The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students when they are off the College site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place out of College, but is linked to membership of the College.

1.2 The College will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of College.

1.3 The policy also covers the contents of, and use of, personal electronic equipment on the College site.

2. ROLES AND RESPONSIBILITIES

The following section outlines the roles and responsibilities for e-safety of individuals and groups within the College:

2.1 **Governors**

Governors are responsible for the approval of the e-safety policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about e-safety incidents and monitoring reports.

2.2 **Head of College and Senior Leaders**

- The Head of College is responsible for ensuring the safety (including e-safety) of members of the College community, though the day-to-day responsibility for e-safety will be delegated to the E-Safety Co-ordinator / Officer.
- The Head of College / Senior Leaders are responsible for ensuring that the E-Safety Coordinator / Officer and other relevant staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, as relevant.
- The Head of College / Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in College who carry out internal e-safety monitoring roles. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Senior Management Team will receive regular monitoring reports from the E-Safety Co-ordinator / Officer.
- The Head of College and another members of the Senior Management Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.
- The Head of College / Senior Leaders to be aware of, and monitor the risk of, radicalisation within the student and staff body. They will ensure staff are trained and regularly updated on this PREVENT duty and will make necessary referrals to 'Channel' about concerns that are presented through the designated PREVENT lead.

2.3 **E-Safety Co-ordinator / Officer:**

- Takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the College e-safety policies / documents.

- Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- Provides training and advice for staff.
- Liaises with the Local Authority.
- Liaises with College ICT technical staff.
- Receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments.
- Attends relevant meeting / committee of Governors.
- Reports regularly to Senior Management Team.

2.4 **Network Manager / Technical staff:**

The IT Manager / ICT Technicians / ICT Co-ordinator is responsible for ensuring:

- That the College's ICT infrastructure is secure and is not open to misuse or malicious attack.
- That the College conforms to any relevant Local Authority E-Safety Policy and guidance.
- That users may only access the College's networks through a properly enforced password protection policy, in which passwords are regularly changed.
- That he / she keeps up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as and when required.
- That the use of the network / Microsoft Teams) / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the E-Safety Co-ordinator / Officer, Head of College, ICT Co-ordinator for investigation / action / sanction.
- That monitoring software / systems are implemented and updated as agreed in College policies.

2.5 **Teaching and Support Staff**

Are responsible for ensuring that:

- They have an up to date awareness of e-safety matters and of the current College e-safety policy and practices.
- They have read and understood the College's Staff ICT Policies.
- They report any suspected misuse or problem to the E-Safety Co-ordinator / Officer, Head of College, ICT Co-ordinator for investigation / action / sanction.
- Digital communications with students / pupils (email / Microsoft Teams / voice) should be on a professional level and only carried out using official College systems.
- E-safety issues are embedded in all aspects of the curriculum and other College activities.
- Students / pupils understand and follow the College e-safety and ICT policies.
- Students / pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- They monitor ICT activity in lessons, extra-curricular and extended College activities.
- They are aware of e-safety issues related to the use of mobile/smart phones, cameras and hand held devices and that they monitor their use and implement current College ICT policies with regard to these devices.
- In lessons where internet use is pre-planned, 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

2.6 **Designated Person for Child Protection / Child Protection Officer**

Should be trained in e-safety issues and be aware of the potential for serious child protection issues to arise from:

- Sharing of personal data.
- Access to illegal / inappropriate materials.
- Inappropriate on-line contact with adults / strangers.

- Potential or actual incidents of grooming.
- Cyber-bullying.

2.7 **Students**

- Are responsible for using the College ICT systems in accordance with the Student ICT Policies, which they will be expected to acknowledge before being given access to College systems.
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Will be expected to know and understand College policies on the use of mobile/smart phones, digital cameras and hand held devices. They should also know and understand College policies on the taking / use of images and on cyber-bullying.
- Should understand the importance of adopting good e-safety practice when using digital technologies out of College and realise that the College's e-safety policy covers their actions out of College, if related to their membership of the College.
- Are responsible for the contents of electronic equipment in their possession on the College site.

2.8 **Parents / Carers**

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The College will therefore take every opportunity to help parents / carers understand these issues through parents' evenings, newsletters, letters, website and information about national / local e-safety campaigns / literature.

3. POLICY STATEMENTS

3.1 **Education – Students**

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 e-safety is therefore an essential part of the College's e-safety provision. Children and young people need the help and support of the College to recognise and avoid e-safety risks and build their resilience.

3.2 E-safety education will be provided in the following ways:

- A planned e-safety programme should be provided as part of ICT / PHSE and should be regularly revisited – this will cover both the use of ICT and new technologies in College and outside College.
- Key e-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 helped to understand the need for the student ICT policies and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside College.
- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Rules for use of ICT systems / internet will be displayed in all rooms.
- Staff should act as good role models in their use of ICT, the internet and mobile devices.

3.3 **Education – Parents / Carers**

Many parents and carers 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 the children's on-line experiences. Parents / Carers often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it.

3.4 The College will therefore seek to provide information and awareness to parents and carers.

3.5 **Education - Extended Schools**

The College will offer family learning presentations in ICT, media literacy and e-safety so that parents / carers and children can together gain a better understanding of these issues. Messages to the public around e-safety should also be targeted towards grandparents and other relatives as well as parents / carers. Everyone has a role to play in empowering children to stay safe while they enjoy these new technologies, just as it is everyone's responsibility to keep children safe in the non-digital world.

3.6 **Education and Training – Staff**

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

- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the College e-safety policy and ICT policies
- This e-safety policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.
- The E-Safety Coordinator (or other nominated person) will provide advice / guidance / training as required to individuals as required.

3.7 **Training – Governors**

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

- Attendance at training provided by the Local Authority / National Governors Association or other relevant organisation.
- Participation in College training / information sessions for staff or parents / carers.

3.8 **Technical – Infrastructure / Equipment, Filtering and Monitoring**

The College will be responsible for ensuring that the College 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 will be effective in carrying out their e-safety responsibilities:

- College ICT systems will be managed in ways that ensure that the College meets the e-safety technical requirements outlined in any relevant Local Authority e-safety policy or guidance.
- There will be regular reviews and audits of the safety and security of College ICT systems.
- Servers, wireless systems and cabling must be securely located and physical access restricted.
- All users will have clearly defined access rights to College ICT systems. Details of the access rights available to groups of users will be recorded by, and be available from the IT Manager.
- All users will be provided with a username and password by the IT Manager. Student users will be required to change their password every 200 days with passwords a minimum of 5 characters long. Staff users are required to change their password every 365 days using one with a minimum of 8 characters and complexity rules.
- All external access to Microsoft 365 for all users (staff and student) must be protected by Multi-Factor Authentication (MFA).

- The ‘administrator’ passwords for the College ICT system, used by the IT Manager and IT technical staff must also be available to the Head of College or other nominated senior leader and kept in a secure place.
- Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- The College maintains and supports web and page content filtering services. In the event of the IT Manager (or other person) needing to switch off the filtering for any reason, or for any user, this must be recorded and agreed for by the E-Safety co-ordinator.
- Any filtering issues should be reported immediately to the IT Manager.
- Requests from staff for websites to be removed from the filtered list will be considered by the IT Manager and if deemed necessary, confirmed with the E-Safety co-ordinator.
- College ICT technical staff regularly monitor and record the activity of users on the College ICT systems and users are made aware of this in the ICT Policies.
- Appropriate security measures are in place to protect the servers, routers, switches, wireless systems and workstations from accidental or malicious attempts which might threaten the security of the College systems and data.
- Agreed staff and student ICT policies are in place regarding the downloading of executable files by users.
- An agreed staff ICT policy is in place regarding the extent of personal use that staff are allowed on laptops and other portable devices that may be used out of College.
- An agreed staff ICT policy is in place that forbids staff from installing programs on College workstations / portable devices without the prior consent of the IT Manager.
- The College infrastructure and individual workstations are protected by up to date virus software.

3.9 **Curriculum**

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages in the use of ICT across the curriculum.

- In lessons where internet use is pre-planned, it is best practice that students 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, eg using search engines, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs, and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the IT Manager (and other relevant IT technical staff) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.
- Students 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.

3.10 **Use of Digital and Video Images - Photographic, Video**

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 and students need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. The College will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet eg on social networking sites.
- Staff are allowed to take digital / video images to support educational aims. Those images should only be taken on College 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 College 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.
- Written permission from parents or carers will be obtained before photographs of students are published on the College website.

3.11 **General Data Protection Principles**

This policy must be read in conjunction with the Four Cs Trust General Data Protection Regulations Policy and the Trust's Staff ICT Policy.

3.12 **Communications**

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

	Staff and other adults				Students			
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/smart phones may be brought to College	X				X			
Use of mobile/smart phones in lessons		X				X		
Use of mobile/smart phones in social time	X				X			
Taking photos on mobile/smart phones or other camera devices	X						X	
Use of personal email addresses on College network				X				X

Use of College email for personal emails				X				X
Use of chat rooms / facilities on College network				X				X
Use of instant messaging on College network				X				X
Use of social networking sites on College network				X				X
Use of blogs on College network		X					X	

3.13 When using communication technologies the College considers the following as good practice:

- The official College email service may be regarded as safe and secure and is monitored.
- Users need to be aware that email communications may be monitored.
- Users must immediately report, to the nominated person (eg class teacher, E-Safety Co-ordinator), the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff and students or parents / carers (email, chat, Microsoft Teams etc) must be professional in tone and content. Personal email addresses, text messaging or public chat / social networking programmes must not be used for these communications.
- Students will be provided with individual College email addresses for educational use.
- Students should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.
- Personal information should not be posted on the College website and only official email addresses should be used to identify members of staff.

3.14 **Unsuitable / Inappropriate Activities**

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

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	child sexual abuse images					X
	promotion or conduct of illegal acts, eg under the child protection, obscenity, computer misuse and fraud legislation					X
	adult material that potentially breaches the Obscene Publications Act in the UK					X
	criminally racist material in UK					X
	pornography				X	
	promotion of any kind of discrimination				X	
	promotion of racial or religious hatred					X
	threatening behaviour, including promotion of physical violence or mental harm					X
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the College or brings the College into disrepute				X	
Using College systems to run a private business					X	
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards the College					X	
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions					X	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)					X	

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

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

3.16 If any apparent or actual misuse appears to involve illegal activity ie
- Child sexual abuse images.
- Adult material which potentially breaches the Obscene Publications Act.
- Criminally racist material.
- Other criminal conduct, activity or materials.

the Head of College and E-Safety Co-ordinator should be informed in the first instance.

3.17 If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (as above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. All relevant information should be passed on to the E-Safety Co-ordinator and Senior Management Team.

3.18 It is more likely that the College 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 College 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 outlined by pastoral and the grid below:

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

Using proxy sites or other means to subvert the College's filtering system	X	X			X	X	X	X	X
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X						X	
Deliberately accessing or trying to access offensive or pornographic material	X	X			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	X	X	X

Staff	**Actions / Sanctions**					
Incidents:	Refer to line Manager	Refer to Head of College	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc.	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
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email						X
Unauthorised downloading or uploading of files						X
Allowing others to access College network by sharing username and passwords or attempting to access or accessing the College network, using another person's account						X
Careless use of personal data eg holding or transferring data in an insecure manner	X					
Deliberate actions to breach data protection or network security rules						X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		X				

Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature		X				
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students		X				
Actions which could compromise the staff member's professional standing						X
Actions which could bring the College into disrepute or breach the integrity of the ethos of the College		X				
Using proxy sites or other means to subvert the College's filtering system						X
Accidentally accessing offensive or pornographic material and failing to report the incident						X
Deliberately accessing or trying to access offensive or pornographic material		X				X
Breaching copyright or licensing regulations						X
Continued infringements of the above, following previous warnings or sanctions		X				X