ANSFORD ACADEMY

LEARNING TOGETHER TO LEAD OUR LIVES

Curriculum, Assessment and Teaching and Learning Policy Suite

E-Safety Code of Practice

(Incorporating Mobile Phone Code of Conduct and Bring Your Own Device Code of Conduct)

Status:	**Non-Statutory**
Adopted:	**May 2023**
Renewal Period:	**3 Yearly**
Next Review:	**May 2026**

Section A: Rationale

The internet and accompanying technologies have become integral to the lives of children and young people in today's society, both within the Academy and in their wider lives. The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and students learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning.

However, the use of these new technologies can put young people at risk within and outside the Academy. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content.
- Unauthorised access to / loss of / sharing of personal information.
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing / distribution of personal images without an individual's consent or knowledge.
- Inappropriate communication / contact with others, including strangers
- Cyber-bullying.
- Access to unsuitable video / internet games.
- An inability to evaluate the quality, accuracy and relevance of information on the internet.
- Plagiarism and copyright infringement.
- Illegal downloading of music or video files.
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

Many of these risks reflect situations in the off-line world and, as with all other risks, it is impossible to completely eliminate those risks. It is therefore essential, through good educational provision, to build students' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in the Academy are bound.

Section B: Monitoring and Review

The Academy will monitor the impact of the policy using:

- Logs of reported incidents.
- Monitoring logs of internet activity (including sites visited).
- Internal monitoring data for network activity.

Section C: Scope of the Policy

This policy applies to all members of the Academy community (including staff, students, governors, volunteers, parents / carers, visitors, community users) who have access to and are users of Academy ICT equipment, both in and out of the Academy. The Education and Inspections Act 2006

empowers the Headteacher, 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 penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy.

Section D: Links to Other Policies

- Anti-Bullying
- Behaviour Management
- Bring Your Own Device Code of Conduct
- Employee Code of Conduct
- Mobile Phone Code of Conduct
- Safeguarding and Child Protection

Section E: Roles and Responsibilities

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

1. **Governors**

   Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy.

2. **Headteacher**

   The Headteacher is responsible for ensuring the safety (including e-safety) of members of the Academy community, though the day-to-day responsibility for e-safety will be delegated to the E-Learning Officer.

   The Headteacher and DSL 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.

   In the event that there are grounds for suspicion of inappropriate use of Academy property or the Academy network by the Headteacher, this should be presented directly to the Chair of Governors who will then consult the E-Learning Officer and ICT Network Manager as appropriate.

3. **Deputy Headteacher: Curriculum and Standards**

   - Has a leading role in establishing and reviewing the Academy e-safety policies/ documents.
   - Ensures the E-Learning Officer and other relevant staff receive suitable Professional Learning to enable them to carry out their e-safety roles and to train other colleagues, as relevant.
   - Ensures the curriculum is fit for purpose and reflects the most recent e-safety developments.
   - Ensures that students are trained in E-safety issues via assemblies and the curriculum.

4. ICT Network Manager

The Network Manager is responsible for ensuring:

- the ICT infrastructure is secure and is not open to misuse or malicious attack.
- they keep 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 relevant.
- the use of the network/Portal/remote access/email is regularly monitored in order that any misuse/attempted misuse can be reported to the E-Learning Officer for investigation.
- that monitoring software/systems are implemented and updated.

5. Designated Safeguarding Lead

- takes day to day responsibility for e-safety issues and has a contributory role in establishing and reviewing the Academy 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 ICT technical staff.
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments.
- provides parents with e-safety information and guidance.

In the event that there are grounds for suspicion of inappropriate use of Academy property or the Academy network by the E-Safety Officer, this should be presented to the Headteacher

In addition, the Designated Safeguarding Lead 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.

6. Teaching and Support Staff

Teaching and Support staff are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current Academy e-safety policy and practices.
- they have read, understood and signed the Academy Staff Acceptable Use Policy (AUP).
- they report any suspected misuse or problem to the E-Learning Officer for investigation.
- digital communications with students should be on a professional level only using the school email systems.
- students understand and follow the Academy e-safety and acceptable use policy.
- students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- they monitor ICT activity in normal lessons, intervention sessions, extracurricular sessions and extended school activities

- they are aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use.
- they do not have contact or 'friend' or 'follow' any current student or contact them via personal email, social media, phone or text.

7. Students

- are responsible for using the Academy ICT systems in accordance with the Student Acceptable Use Policy set out in the Academy planner.
- 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 academy policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand Academy 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 both inside and outside of the Academy

8. Parents and Carers

Parents and 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 Academy will therefore take every opportunity to help parents understand these issues through a variety of means such as: the Academy website, parents' evenings, advice sessions, newsletters, letters and through providing information about national/local e-safety campaigns.

Parents and carers will be responsible for supporting the Student Acceptable Use Policy.

Section F: Communication Technologies

A wide range of rapidly developing communications technologies has the potential to enhance learning.

The following table shows how the Academy currently considers the benefit of using these technologies for education outweighs their risks and disadvantages:

	Staff & other stakeholders				Students			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permissio	Not allowed
Mobile phones may be brought to Academy	X					X		
Use of mobile phones in lessons		X					X	
Use of handheld devices in lessons	X				X			
Use of mobile phones/handheld devices in social time	X							X
Taking photos on personal mobile phones or other camera devices				X			X	
Use of personal email addresses in Academy, or on Academy network				X				X
Use of Academy email for personal emails	X				X			
Use of chat rooms / facilities			X					X
Use of instant messaging			X				X	
Use of social networking sites			X					X
Use of blogs		X				X		

*Allowed at certain times means: when it is deemed reasonable for educational or Academy purposes.

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

- The official Academy email service may be regarded as safe and secure and is monitored. Staff and students should therefore use only the Academy email service to communicate with others when in Academy, or on Academy systems (e.g. by remote access).
- Staff are permitted to use the school mail for personal emails within break times. However, the content of the email must not bring the Academy into disrepute; this includes anything

of a libellous, defamatory or criminal nature. Staff should also be aware that the contents of their email may be monitored.

- Users need to be aware that email communications may be monitored
- Users must immediately report to the E-Learning Officer, in accordance with the Academy policy, if 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 (e.g. Email must be professional in tone and content using school email and telephone systems only)
- 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 Academy website and only official email addresses should be used to identify members of staff.

Section G: Social Media

Social media such as Facebook, Twitter TikTok, and a large number of other providers, play an increasingly prevalent part in online communication. Due to the open and highly varied nature of content on these sites they are not accessible within the Academy and staff should not seek to access them. Staff may wish to access their own social media accounts on Academy equipment through their home network. This falls under appropriate personal usage. Irrespective of the equipment used to access social media there are a number of issues for staff to be aware of to ensure that they remain safe online:

- Social Networking sites are not always private and secure by default. Staff should make sure that all privacy settings are correctly applied and check regularly to ensure that they are up to date regarding any changes that affect their security. If in doubt, they should seek advice from the ICT Network Manager.
- Staff should not seek or accept any contact from current students and it is inadvisable to seek or accept contact from past students who may have existing students in their network as this could easily allow them to access their profile, photos, posts, etc.
- If under 18s are on a staff member's friend list (perhaps family members) be especially careful that the content posted is appropriate, including photos.
- As part of maintaining an appropriate professional character it is strongly advised that staff avoid bad language, sexual connotations and obscene jokes.
- Staff should take into account the potentially serious effects of discussing issues, even in an implied sense, relating to the Academy, its staff or its learners, in the public forum of social media. In a more general sense staff should be aware that once a comment or photograph has been published online it will remain so and *could* cause significant offence or embarrassment at any point in the near or distant future. This is likely to lead to disciplinary proceedings and in extreme cases legal sanction.

The Academy has a registered Twitter account (@AnsfordAcademy) that is used to communicate information in a timely and accessible fashion (for instance Academy closures due to poor weather). Should staff wish to use this to communicate with the Academy's community they should email the ELearning Officer with the content they wish to be sent out.

Should any member of staff wish to create a social media profile that is in any way linked to the Academy, its learners or staff, they must discuss this with the ICT Network Manager and E-Learning Officer who will advise.

Section H: Unsuitable and/or Inappropriate Activities

The following table outlines user actions and whether or not they are acceptable:

User Actions		Acceptable	Acceptable at certain	Acceptable for nominated users	Unacceptable	Unacceptable and illega
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate 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 Academy or brings the Academy into disrepute				X	
Using Academy systems to run a private business					X	
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the Academy					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			
Legal file sharing	X				
Use of social networking sites			X		
Use of video broadcasting e.g. YouTube	X				

Section I: Responding to Incidents of Misuse

It is hoped that all members of the Academy 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.

If any apparent or actual misuse appears to involve illegal activity i.e. :

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

the Academy will follow the appropriate safeguarding procedures and contact the appropriate bodies accordingly.

Section J: Student Actions and Consequences

(*) the E-Safety Officer will work closely with the designated safeguarding officer in all matters involving child protection issues. **Incidents:**	Refer to class teacher / tutor	Refer to HOY	Refer to ELearningOfficer (*)	Refer to DSL	Refer to Principal and Police	Refer to technical support staff for actionfiltering / security etc.	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction e.g. detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X		X		X			X
Incidents where there are allegations of Child Protection issues			X	X		X				
Unauthorised use of non-educational sites in lessons	X					X			X	
Unauthorised use of mobile phone / digital camera / other handheld device	X								X	
Unauthorised use of social networking / instant messaging / personal email	X					X			X	
Unauthorised downloading or uploading of files						X			X	
Allowing others to access Academy network by sharing username and passwords		X				X			X	

Attempting to access or accessing the Academy network, using another student's / student's account		X				X			X	
Attempting to access or accessing the Academy network, using the account of a member of staff			X			X				X
Corrupting or destroying the data of other users		X				X				X
Sending an email, text or instant message regarded as offensive, harassment or of a bullying nature		X								X
Continued infringements of the above, following previous warnings or sanctions			X							X
Actions which could bring the Academy into disrepute or breach the integrity of the ethos of the Academy			X							X
Using proxy sites or other means to subvert the Academy's filtering system			X			X				X
Accidentally accessing offensive or pornographic material		X		X		X			X	
Deliberately accessing or trying to access offensive or pornographic material			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	

Section K: Staff Actions and Consequences

Incidents:	Refer to Line Manager		Refer to Principal	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).			X	X	X			X	X
Excessive or inappropriate personal use of the internet / (including inappropriate content on social networking sites / instant messaging) use of personal email within the Academy	X					X			

Unauthorised downloading or uploading of files	X					X			
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	X					X			
Careless use of personal data e.g. holding or transferring data in an insecure manner			X			X	X		
Deliberate actions to breach data protection or network security rules			X			X	X		
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software			X			X			X
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature or in any other way considered inappropriate within a working environment.			X						X
Using personal email / social networking / instant messaging / text messaging to carry out digital communications with students, or the wider public about matters relevant to their employment.	X								
Actions which could compromise the staff member's professional standing			X				X		
Actions which could bring the Academy into disrepute or breach the integrity of the ethos of the Academy			X				X		
Using proxy sites or other means to subvert the Academy's filtering system			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
Breaching copyright or licensing regulations			X			X			
Continued infringements of the above, following previous warnings or sanctions			X					X	X

ANSFORD ACADEMY

LEARNING TOGETHER TO LEAD OUR LIVES

Mobile Phone Code of Conduct

1. Introduction

a) Students benefit from having access to mobile phones for reasons of safety. Whilst they play a part in social networking their use in this context can be both useful but also unhelpful.

b) Mobile phones are not considered to be a learning tool and therefore should not be used as such.

c) The rules governing the use of mobile phones in the Academy have been drawn up in the context outlined above.

2. Guidelines

a) Students are allowed to bring mobile phones to school unless they have been informed by a member of the Leadership Team to the contrary.

b) Mobile phones are not to be used during academy lesson time without the permission of a teacher.

c) Students are not permitted to contact parents during the Academy day or on an Academy visit unless they have specific permission from a teacher.

d) Students caught using a mobile phone during Academy lessons without the permission of a teacher will have the phone confiscated. It will be held in the Academy office for collection at the end of the day. Except in exceptional circumstances, the mobile phone will always be returned on the same day it was confiscated.

e) Where students use mobile phones out of Academy hours to bully or intimidate another student it will be regarded as effectively bullying within the Academy community. It will be dealt with as such.

f) Where a student persistently breaches the Academy rules on the use of mobile phones they will be banned from bringing them onto site.

3**. Links with other Policies:**

- Anti-Bullying
- Behaviour Management
- Bring Your Own Device
- E-Safety
- Safeguarding and Child Protection

ANSFORD ACADEMY

LEARNING TOGETHER TO LEAD OUR LIVES

Bring Your Own Device (BYOD) Code of Conduct

1. Introduction

a) As part of our curriculum students will benefit from having access to handheld devices. These devices are for educational use and to support the learning which takes place in lessons. Please note that it is not compulsory for any student to have their own device to access the curriculum.

b) The rules governing use of handheld devices in the Academy have been drawn up in the context outlined above.

c) Handheld devices constitute as laptops, tablets and notebooks. Mobile Phones are not considered as a learning tool and therefore are subject to rules stated in the Mobile Phone Policy.

2. Guidelines

a) Students are allowed to bring handheld devices to school unless they have been informed by a member of the Leadership Team to the contrary.

b) Handheld devices may be used in Academy lessons at the discretion of the teacher.

c) Students caught using their hand held devices inappropriately during the Academy day may have the device confiscated. It will be held in the Academy office for collection at the end of the day. Except in exceptional circumstances the hand held device will always be returned on the same day it was confiscated.

d) Where students use hand held devices out of Academy hours to bully or intimidate another student it will be regarded as effectively bullying within the Academy community. It will be dealt with as such.

e) Where a student persistently breaches the Academy rules on the use of handheld devices they will be banned from bringing them onto site.

3. Operational

a) Students should ensure that all handheld devices are fully charged before each academy day. Students will not be permitted to charge their device in school.

b) When using their handheld devices students are encouraged to use the Academy wifi and the use of 3G or 4G signals is strongly discouraged.

c) All handheld devices should be installed with up to date virus protection and security updates should be downloaded regularly.

d) Hand held devices are brought onto the Academy site at students' own risk. The Academy will not take any responsibility for loss or damage to a hand held device. All Parents/Carers should ensure that their child's device is covered by their own insurance.

This policy is written in conjunction with the E-Safety Code of Practice, the Mobile Phone Code of Conduct and Acceptable Use Policy (AUP) as part of the Safeguarding and Child Protection Suite of policies.