St Andrew's C. Of E. Primary School

ICT E Safety Policy

Policy Number	T5
Target Audience	Staff, Parents and Pupils
Approving Committee	Executive Committee
Last Review Date	Feb 2026
Next Review Date	Feb 2027
Policy Author	Gemma Wallace

Version Control			
Version No	**Date Approved**	**Reviewed By**	**Changes**
V1			
V2		J Squires	Reference made to school photo policy
V3		J Squires	Summary of filtering and monitoring included Pupil AUP form removed
V4		**JS**	**Updated names of key staff. P15 wording**
V5		**TH**	Updated names of key staff. P. 29 terrorist/extremist material policy added.
V6		**TH**	ICT Safety Manager Review date Whole school consultation (staff meetings)
V6		**TH**	Separate E Safety policy created for Covid19 home learning guidance. Found under Staff Resources > Policies – Teaching > Safeguarding Online teaching and learning policy 20-21
V7		**GW**	Updated names of key staff. Page 5 – dates updated. Review dates added Page 6 – RM Safety Net checks added Page 8 – pupils section – children's AUP from Sept 2023 Page 9 – e-safety given high priority Page 10 – social media staff – school twitter account allowed only Page 11 – phones/tablets etc not allowed on school toy days
V8		**GW**	Page 10 & 11 – updated to reflect use of smart watches and other digital devices.
V9		**GW**	Updated mentions of mobile phones to bring this policy in line with the new mobile phone policy

Contents

Introduction

The School E-Safety Policy applies to all members of the school community (including staff, students/pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of school ICT systems and mobile technologies, both in and out of school.

Policy Governance

Development, Monitoring and Review of this Policy

The e-Safety policy is post of the School Development Plan and relates to other policies including those for ICT, anti-bullying and safeguarding.

Miss Gemma Wallace is the school's e-Safety coordinator who will work in collaboration with the designated safeguarding lead, Mr Mike Platt (Head teacher).

Our e-Safety policy has been written by the school, building on the Salford e-Safety Policy template. It has been agreed by senior management and approved by governors

The e-Safety policy and its implementation will be reviewed annually by the computing subject lead and every 3 years by the GB or in response to an incident.

Position	Name(s)
School E-Safety Coordinator	Gemma Wallace
Headteacher	Mike Platt

Consultation with the whole school community has taken place through the following:

Staff meetings/INSET day(s)	September 2022
Governors meeting	3 yearly
School website / newsletters	On- going and regular

Schedule for Review

The implementation of this e-safety policy will be monitored by:	*Gemma Wallace, E-Safety Coordinator* *Mike Platt, Head teacher* *Senior Leadership Team*
Monitoring will take place at regular intervals:	*At least once a year or in response to an incident.*
The *Governing Body* will receive a report on the implementation of the e-safety policy generated by the subject leader at regular intervals-termly:	*Termly-in the TLR report*
The E-Safety Policy will be reviewed *annually*, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place. The next anticipated review date will be:	*June 2024*
Should serious e-safety incidents take place, the following external persons / agencies should be informed:	*LA ICT Manager* *LA Designated Officer on* 0161 603 4350

Scope of the Policy

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

Roles and Responsibilities

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

Governors:

- Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy.
- A designated governor (Emma Fahy) reviews our filtering system logs with Headteacher/e-safety coordinator. Records of these checks are kept.

Headteacher and Senior Leaders:

- The Headteacher is responsible for ensuring the safety (including e-safety) of members of the school community
- The Headteacher and another member of the Senior Leadership Team/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 Headteacher regularly reviews our filtering system, RM safety net. Records of these checks are kept.

E-Safety Coordinator/Officer:

leads the e-safety committee and/or cross-school initiative on e-safety

- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school 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
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments
- reports regularly to Senior Leadership Team
- regularly checks our filtering system, RM Safety Net, keeping records of these checks.

Network Manager / Technical staff:

The Managed Service provider is responsible for ensuring:

- that the school's ICT infrastructure is secure and is not open to misuse or malicious attack
- that the school meets the e-safety technical requirements outlined in the Salford City Council Security Policy and Acceptable Usage Policy and any relevant Local Authority E-Safety Policy and guidance
- that users may only access the school's networks through a properly enforced password protection policy

Appropriate filtering for Education Settings

Our Safeguarding responsibilities in regards to 'Appropriate' Filtering and Monitoring are supported by RM and SCC. It is important to recognise that no filtering systems can be 100% efficient and need to be supported with good teaching and learning practice and effective supervision.

RM, as filtering providers, ensure that access to illegal content is blocked by

- being IWF members
- blocking access to illegal images by actively implementing the IWF CAIC list
- integrating the 'police assessed list of unlawful terrorist content on behalf of the Home Office'

Full details can be found at RM Provider Checklist Responses

Please also see our Filtering Policy (RM).

Teaching and Support Staff

are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices
- they have read, understood and signed the school Staff Acceptable Use Policy/Agreement (AUP)
- they report any suspected misuse or problem to the E-Safety Co-ordinator, class teacher or Headteacher for investigation/action/sanction

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

Students/pupils:

- are responsible for using the school ICT systems and mobile technologies in accordance with the Student / Pupil Acceptable Use Policy and mobile phone policy. Children will be made aware of an age appropriate AUP each September. This will be repeated annually. The children's AUP is written in child friendly language. A simplified version will be shared with EYFS children at the start of each academic year.
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so

Parents/Carers

The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website/Learning Platform and information about national/local e-safety campaigns/literature. Parents and carers will be responsible for:

- accessing the school ICT systems or Learning Platform in accordance with the school Acceptable Use Policy.

Community Users

Community Users who access school ICT systems or Learning Platform as part of the Extended School provision will be expected to sign a Acceptable Use Policy (AUP) before being provided with access to school systems.

E-Safety Education and Training

Education – students / pupils

E-Safety education will be provided in the following ways:

- A planned e-safety programme will be provided as part of Computing/PHSE/other lessons and will be regularly revisited – this will cover both the use of ICT and new technologies in and outside school
- E-safety is given high priority in school. Each year group are taught about e-safety at least three times per year, in addition to whole school assemblies.
- Key e-safety messages will be reinforced as part of a planned programme of assemblies and tutorial/pastoral activities
- Students/pupils will 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

Education & 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 will receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Policies

Communication devices and methods

The following table shows the school's policy on the use of communication devices and methods.

Where it is indicated that the method or device is allowed at certain times, these are clearly outlined in the next table.

	Staff & other adults				Students/Pupils			
Communication method or device	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
	☑	⚠	⚠	☒	☑	⚠	⚠	☒
Mobile phones may be brought to school	☑						☑ Y6 chn. Kept in bags.	
Use of mobile phones in lessons				☒				☒
Use of mobile phones/Smart Watches in social time	☑							☒
Taking photos on personal mobile phones or other camera devices		⚠						☒
Taking photos on school devices (inc iPads)	☑				☑ As part of class work			
Use of personal hand held devices eg PDAs, PSPs		⚠				⚠	⚠	

Use of personal email addresses in school, or on school network	☑							☒
Use of school email for personal emails				☒				☒
Use of chat rooms / facilities				☒				☒
Use of instant messaging				☒				☒
Use of social networking sites		(twitter – school account)						☒
Use of blogs	☑							

This table indicates when some of the methods or devices above may be allowed:

	Circumstances when these may be allowed	
Communication method or device	**Staff & other adults**	**Students/Pupils**
Use of mobile phones/digital devices inc smart watches in social time	during breaks or after school/non contact time	not allowed
Taking photos on personal mobile phones, digital devices, smart watches or other camera devices.	only if school device is unavailable. All photos must be uploaded and deleted from the device as soon as possible. For further clarification, please consult the photos policy	Not allowed – staff remind children not to being in phones/tablets/other electronic devices on toy days
Use of personal hand held devices eg PDAs, PSPs	when used as part of a lesson or during non-teaching time	when used as part of a lesson – school devices
Use of personal email addresses in school, or on school network	during breaks or after school. Can be used if staff are having difficulties with their work email.	not allowed

Use of school email for personal emails	not allowed	not allowed
Use of chat rooms / facilities	not allowed on school network. Access from own devices allowed during breaks or outside the teaching day.	not allowed
Use of instant messaging	not allowed on school network. Access from own devices allowed during breaks or outside the teaching day.	not allowed
Use of social networking sites	not allowed on school network. Access from own devices allowed during breaks or outside the teaching day. School twitter account is allowed.	not allowed
Use of blogs	Blogs can be used by teaching staff.	Not allowed

Unsuitable/inappropriate activities

The school 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 school or outside school when using school equipment or systems. The school policy restricts certain internet usage as follows:

	Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
User Actions	☑			☒	☒
child sexual abuse images					☒
promotion or conduct of illegal acts, eg under the child protection, obscenity, computer misuse and fraud legislation					☒
adult material that potentially breaches the Obscene Publications Act in the UK					☒
criminally racist material in UK					☒
Pornography					☒
promotion of any kind of discrimination					☒
promotion of racial or religious hatred					☒
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 school or brings the school into disrepute				☒	
Using school systems to run a private business				☒	
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by SCC and / or the school				☒	
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 (eg 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 gaming (educational)					
On-line gaming (non educational)					
On-line gambling					
On-line shopping / commerce					
File sharing					
Use of social networking sites					
Use of video broadcasting eg Youtube					
Accessing the internet for personal or social use (e.g. online shopping)					
Using external data storage devices (e.g. USB) that have not been encrypted (password protected and checked for viruses					

Good practice guidelines

Email

Images, photos and videos

Internet

Mobile phones

Social networking (e.g. Facebook/ Twitter)

.

Webcams

Incident Management

Incidents (students/pupils):	Refer to class teacher	Refer to Headteacher	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)	☑	☑			☑		☑	☑
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 school network by sharing username and passwords	☑	☑		☑			☑	
Attempting to access or accessing the school network, using another student's/pupil's account	☑	☑		☑			☑	
Attempting to access or accessing the school 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 school into disrepute or breach the integrity of the ethos of the school	☑	☑			☑	☑		☑
Using proxy sites or other means to subvert the school's filtering system	☑	☑		☑	☑	☑		☑
Accidentally accessing offensive or pornographic material and failing to report the incident	☑						☑	
Deliberately accessing or trying to access offensive or pornography	☑	☑		☑		☑		☑
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	☑	☑					☑	

Incidents (staff and community users):	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering / security etc	Removal of network / internet access rights	Warning	Further sanction
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities)	☑	☑			☑	disciplinary
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email	☑				☑	disciplinary

Unauthorised downloading or uploading of files	☑		☑		☑	
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	☑		☑		☑	disciplinary
Careless use of personal data eg holding or transferring data in an insecure manner	☑				☑	
Deliberate actions to breach data protection or network security rules	☑		☑		☑	disciplinary
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	☑		☑		☑	disciplinary
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	☑		☑		☑	gross disciplinary
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils	☑		☑		☑	
Actions which could compromise the staff member's professional standing	☑				☑	gross disciplinary
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	☑				☑	

Using proxy sites or other means to subvert the school'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	☑				☑	

Further information and support

For a glossary of terms used in this document:

http://www.salford.gov.uk/d/salford-esafety-glossary-jan2012.pdf

For e-Safety Practice Guidance for those who Work and Volunteer with, and have a Duty of Care to Safeguard Children and Young People:

http://www.salford.gov.uk/d/e-Safety-Practice-Guidance.pdf

R u cyber safe?

E-safety tips about how to stay safe online:

http://www.salford.gov.uk/rucybersafe.htm

I

Appendix 1 – Staff, Volunteer, Community User AUP

Staff, Volunteer and Community User Acceptable Use Policy Agreement Template

School Policy

This Acceptable Use Policy (AUP) is intended to ensure:

- that staff, volunteers and community users will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff, volunteers and community users are protected from potential risk in their use of ICT in their everyday work.

The school will try to ensure that staff, volunteers and community users will have good access to ICT to enhance their work, to enhance learning opportunities for pupils' learning and will, in return, expect staff, volunteers and community users to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that students/pupils receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed e-safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of school ICT systems (eg laptops, email, VLE etc) out of school.
- I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password.

- I will immediately report any illegal, inappropriate or harmful material or incident become aware of, to the appropriate person.

- I will ensure that children are safe from terrorist and extremist material when accessing the internet in school.

I will be professional in my communications and actions when using school ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.

- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.

- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital/video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (eg on the school website / VLE) it will not be possible to identify by name, or other personal information, those who are featured.

- I will only use chat and social networking sites in school in accordance with the school's policies.

- I will only communicate with students/pupils and parents/carers using official school systems. Any such communication will be professional in tone and manner.

- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my personal hand held/external devices (PDAs/laptops/USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules in line with the School's E-Safety Policy set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.

- I will only use personal email addresses on the school ICT systems under the circumstances set out in the School's E-Safety policy.

- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.

- I will ensure that my data is regularly backed up, in accordance with relevant school policies.

- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.

- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.

- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless I have specific permission to do so.

- I will not disable or cause any damage to school equipment, or the equipment belonging to others.

- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School/Local Authority Personal Data Policy .Where personal data is transferred outside the secure school network, it must be encrypted.

- I understand that data protection policy requires that any staff or student / pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.

- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work.

- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

Staff, Volunteer and Community User Acceptable Use Agreement Form

This form relates to the student/pupil Acceptable Use Policy (AUP), to which it is attached.

I understand that I am responsible for my actions in and out of school:

- I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment out of school and my use of personal equipment in school or in situations related to my employment by the school.

- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and/or the Local Authority and in the event of illegal activities the involvement of the police

- **I have read and understood the School's E-safety Policy**

I have read and understand the above and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Name	
Position	
Signed	
Date	

Appendix 2 – Use of Images Consent Form

Use of Digital / Video Images

The use of digital/video images plays an important part in learning activities. Students/Pupils and members of staff may be using digital or video cameras to record evidence of activities in lessons and out of school. These images may then be used in presentations in subsequent lessons.

Images may also be used to celebrate success through their publication in newsletters, on the school website and occasionally in the public media,

The school will comply with the Data Protection Act and request parents' / carers' permission before taking images of members of the school. We will also ensure that when images are published that the young people cannot be identified by the use of their names.

Parents are requested to sign the permission form below to allow the school to take and use images of their children.

Permission Form

Parent / Carers Name	
Student / Pupil Name	

As the parent / carer of the above student / pupil, I agree to the school taking and using digital / video images of my child / children. I understand that the images will only be used to support learning activities or in publicity that reasonably celebrates success and promotes the work of the school.

I agree that if I take digital or video images at, or of, school events which include images of children, other than my own, I will abide by these guidelines in my use of these images.

Signed	
Date	

Appendix 3 – Children's AUP

Pupil User Acceptable Use of ICT Agreement

September 2023

I understand that I am responsible for my actions in and out of school.

I agree to be kind and considerate online in and out of school.

I will behave in a responsible way online in and out of school.

I will not post photos of people online without their permission.

I will respect all ICT equipment in school, such as iPads, laptops and Chromebooks, treating them with care.

If I see something online that worries me, I will tell a trusted grown-up straight away. If this happens in school, I will tell a teacher or teaching assistant.

My school will monitor my use of ICT. This means my teachers can see which websites I have been on.

I understand that the laptops/iPads/Chromebooks in school are to help me with my school work.

I will not share my password with anyone else.

I will not try to use anyone else's username and password.

Signed:

Full name:

Class:

Appendix 4 – Children's AUP (EYFS – children not required to sign)

Pupil User Acceptable Use of ICT Agreement

September 2023

EYFS

I will take care of the laptops and iPads in my classroom.

If I see something online that upsets me, I will tell a grown-up.

I will be kind online.

Laptops and iPads in school help me with my learning.