



Online Safety Policy

This Online Safety Policy was approved by the Governing Body on:	July 2016 M. Grogan (Headteacher) Theresa Taylor (Chair of Governors)
The implementation of this Online Safety Policy will be monitored by the:	Computing Co-ordinator Senior Leadership Team
Monitoring will take place at regular intervals:	Termly
The Governing Body will receive a report on the implementation of the Online Safety Policy generated by the monitoring group at regular intervals:	Annual
The Online 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:	July 2017

Scope of the Policy

This policy applies to all members of the school community (including staff, students/pupils, Governors, 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 Online Safety Policy and for reviewing the effectiveness of the policy.

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.

Computing/E-Safety Coordinator:

- 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;

'Never settle for less than your best'

- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments;
- reports regularly to Senior Leadership Team.

Network Manager / Technical staff:

Computing Technician and Computing Co-ordinator is responsible for ensuring:

- that the school's computing infrastructure is secure and is not open to misuse or malicious attack;
- that the school meets the e-safety technical requirements outlined in any relevant Local Authority E-Safety Policies and guidance;
- that users may only access the school's networks through a properly enforced password protection policy.

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 /Headteacher/ Computing Co-ordinator for investigation/action/sanction.

Designated person for child protection/Child Protection Officer:

will 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 computing systems and mobile technologies in accordance with the Student/Pupil Acceptable Use Policy, which they will be expected to sign before being given access to school systems (NB. at KS1 it would be expected that parents/carers would sign on behalf of the pupils);
- 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 and information about national/local e-safety campaigns/literature. Parents and carers will be responsible for:

- endorsing (by signature) the Student/Pupil Acceptable Use Policy;
- accessing the school computing systems or Learning Platform in accordance with the school Acceptable Use Policy.

Community Users:

Community Users who access school computing systems as part of any Extended School provision will be expected to sign a Community User Acceptable Use Policy (AUP) before being provided with access to school systems.

E-Safety Education and Training

Education – pupils

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

- A planned e-safety programme will be provided as part of Computing/PHSE and will be regularly revisited – this will cover both the use of Computing and new technologies in and outside school;
- 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;
- Updates from Computing/Child Protection Co-ordinator following training sessions.

'Never settle for less than your best'































Social Media

Twitter – All school Twitter users must ensure children under the age of 13 are not following their account. This essentially means that only parents/carers from school should be following the Twitter account.

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.

Communication method or device	Staff & other adults				Students/Pupils			
	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								
Use of mobile phones in lessons								
Use of mobile phones in social time								
Taking photos on other camera devices								
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								
Use of blogs								

'Never settle for less than your best'























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

Communication method or device	Circumstances when these may be allowed	
	Staff & other adults	Students/Pupils
Mobile phones may be brought to school		If children are walking home on own – all mobile phones must be kept in the school office throughout the school day.
Taking photos on other camera devices	During school visits/trips/events	Use for curriculum activities under supervision of staff.
Use of personal hand held devices eg PDAs, PSPs	Use for curriculum activities and during visits/trips/events	Use for curriculum activities under supervision of staff.
Use of personal email addresses in school, or on school network	For communication/ ordering for school business.	
Use of chat rooms / facilities	For educational purposes only eg e-safety lessons	Use for curriculum activities under supervision of staff.
Use of instant messaging		
Use of social networking sites	Twitter can be used to share information about school but only adults can follow school twitter accounts	
Use of blogs		

'Never settle for less than your best'

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 for school purposes					

'Never settle for less than your best'

File sharing					
Use of social networking sites for school purposes					
Use of video broadcasting eg Youtube for school purposes					
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)					

'Never settle for less than your best'

Appendix 1 - Good practice guidelines


Email



DO

Staff and students/pupils should only use their school email account to communication with each other or for school use.





Check the school e-safety policy regarding use of your school email or the internet for personal use e.g. shopping.



DO NOT

Staff: don't use your personal email account to communicate with students/pupils and their families without a manager's knowledge or permission – and in accordance with the e-safety policy.

'Never settle for less than your best'


Images, photos and videos



✓ DO

Only use school equipment for taking pictures and videos.





Check the e-safety policy for any instances where using personal devices may be allowed.

Always make sure you have the Headteacher/SLT knowledge or permission

Make arrangements for pictures to be downloaded to the school network immediately after the event.



✗ DO NOT

Don't download images from organisation equipment to your own equipment.

Don't use your own equipment without Headteacher/SLT knowledge or permission – and in accordance with the e-safety policy.

'Never settle for less than your best'


Internet



✓DO

Understand how to search safely online and how to report inappropriate content .





Staff and students/pupils should be aware that monitoring software will log online activity.

Be aware that keystroke monitoring software does just that. This means that if you are online shopping then your passwords, credit card numbers and security codes may all be visible to the monitoring technicians.



✗DO NOT

Remember that accessing or downloading inappropriate or illegal material may result in criminal proceedings

Breach of the e-safety and acceptable use policies may result in confiscation of equipment, closing of accounts and instigation of sanctions.

'Never settle for less than your best'


Mobile phones



✓DO

Make sure you know about inbuilt software/ facilities and switch off if appropriate.





Check the e-safety policy for any instances where using personal phones may be allowed.

Staff: Make sure you know how to employ safety measures like concealing your number by dialing 141 first



✗DO NOT

Staff: Don't use your own phone without the Headteacher/SLT knowledge or permission.

'Never settle for less than your best'

Social networking (e.g. Facebook/ Twitter)




✓ DO

If you have a personal account, regularly check all settings and make sure your security settings are not open access.

Ask family and friends to not post tagged images of you on their open access profiles.





Don't accept people you don't know as friends.

Be aware that belonging to a 'group' can allow access to your profile.



✗ DO NOT

Don't have an open access profile that includes inappropriate personal information and images, photos or videos.

Staff:

- Don't accept students/pupils or their parents as friends on your personal profile.
- Don't accept ex-students/pupils users as friends.

'Never settle for less than your best'

Webcams

Best practice

DO

Make sure you know about inbuilt software/facilities and switch off when not in use.

Safe practice



Check the e-safety policy for any instances where using personal devices may be allowed.

Always make sure you have the Headteacher/SLT knowledge or permission

Make arrangements for pictures to be downloaded to the school network immediately after the event.

Delete images from the camera/device after downloading.

Poor practice

DO NOT

Don't download images from school equipment to your own equipment.

Don't use your own equipment without Headteacher/SLT knowledge or permission – and in accordance with the e-safety policy.

'Never settle for less than your best'

Incident Management

Incidents (pupils):	Refer to class teacher	Refer to ICT Co-ordinator	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 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									

'Never settle for less than your best'

Incidents (staff and community users):	Refer to ICT Co-ordinator	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/disciplinary
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 school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account							
Careless use of personal data eg 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 pupils							
Actions which could compromise the staff member's professional standing							
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							

'Never settle for less than your best'

Appendix 2

Pupil Acceptable Use Policy Agreement

KS2

This Acceptable Use Policy is intended to make sure:

- That you will be a responsible user and stay safe while using the internet and other technology for learning and personal use
- That ICT systems and users are protected from accidental or deliberate misuse

The school will try to ensure that you will have good access to ICT to enhance your learning and will, in return, expect you to agree to be a responsible user.

Please make sure you read and understand the following

WILL and

WILL NOT statements.

If there's anything you're not sure of, ask your teacher.

'Never settle for less than your best'

I WILL:

- not share my username or password, or try to use any other person's username and password
- immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it online
- respect others' work and property and will not access, copy, remove or change anyone else's files, without their knowledge and permission
- be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions
- hand my mobile phone in to the school office at the start of the day if I have to bring it to school
- understand that, if I do use my own devices in school with teacher permission, I will follow the rules set out in this agreement, in the same way as if I was using school equipment
- immediately report any damage or faults involving equipment or software, however this may have happened
- only use chat and social networking sites with permission during lesson times.

I WILL NOT:

- try (unless I have permission) to make downloads or uploads from the Internet
- take or share images (pictures and videos) of anyone without their permission
- use the school ICT systems for online gaming, internet shopping, file sharing, or video broadcasting (eg YouTube), unless I have permission of a member of staff to do so.
- try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others
- 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
- open any attachments to emails, unless I know and trust the person/organisation who sent the email, due to the risk of the attachment containing viruses or other harmful programmes
- attempt to install programmes of any type on a machine, or store programmes on a computer
- try to alter computer settings

'Never settle for less than your best'

Pupil Acceptable Use Policy Agreement

Foundation Stage & KS1

This Acceptable Use Policy is intended to make sure:

- That you will be a responsible user and stay safe while using the internet and other technology for learning and personal use
- That ICT systems and users are protected from accidental or deliberate misuse

The school will try to ensure that you will have good access to ICT to enhance your learning and will, in return, expect you to agree to be a responsible user.

Please make sure you read and understand the following statements. If there's anything you're not sure of, ask your teacher.

- We only use the internet when an adult is with us.
- We can click on the buttons when we know what they do.
- We always ask if we get lost on the internet.
- We can send and open e-mails together.
- We never give out personal information or passwords.
- We only use computers or ICT equipment with an adult's permission.

Pupil Acceptable Use Agreement Form Template

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

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

- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information)
- I understand that if I fail to follow this Acceptable Use Policy Agreement, I will be subject to disciplinary action. This may include loss of access to the school network/internet, contact with parents and in the event of illegal activities involvement of the police

I have read and understand the above and agree to follow these guidelines when:

- I use the school ICT systems and equipment (both in and out of school)
- I use my own equipment out of school in a way that is related to me being a member of this school e.g. communicating with other members of the school, accessing school email, website etc

(Parents/carers are requested to sign the permission form below to show your support of the school in this important aspect of the school's work).

Name of Pupil		
Group/Class		
Signed (Pupil)		Date
Signed (Parent/Carer)		Date

'Never settle for less than your best'

Staff, Volunteer and Community User Acceptable Use Policy Agreement Template

School Policy

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

- that 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 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, 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 I become aware of, to the appropriate person.

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) 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 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/mobile phones/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.

'Never settle for less than your best'

- 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 disable or cause any damage to school equipment, or the equipment belonging to others.
- 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.

Staff, Volunteer and Community User Acceptable Use Agreement Form

This form relates to the staff, volunteer and community user 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 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	

'Never settle for less than your best'

Appendix 4 – Parental Consent Form (covering letter)

Dear parents/carers,

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. If this happens then when images are published, we will ensure that the young people cannot be identified by the use of their names.

As part of our school E-safety policy, we are asking you to sign the permission form attached, to allow the school to take and use images of your child, and return it to your child's teacher in school by **Wednesday 20th July 2016.**

This is so that we can start to include more images on displays around school and on our school website. In having just one slip to complete, this will also reduce the number of further photograph permission slips that will be required to be sent out by school in the future.

Please be aware that permission slips will continue to be sent out when the 'official' school photographer comes to school to take individual and whole class photographs (October and March each year) as we receive a variety of requests with these photos.

Please also ensure that you complete the ATSA (Atherton and Tyldesley Sports Association) part to the form. There are many sporting events planned for this year for both KS1 and KS2 children and there is every possibility that your child may be selected to represent our school at these events.

Should you have any further questions then please do not hesitate to contact me in school.

Yours Sincerely



Mr M Grogan
Headteacher

'Never settle for less than your best'

Appendix 4 – Parental Consent Form (covering letter)

CONSENT FORM FOR PHOTOGRAPHY AND FILMED IMAGES

(September 2016 – July 2017)

Name of child: _____

Class: _____

As the parent/carer of the above pupil, I agree to the school taking and using digital/video images of my child in the circumstances indicated below. 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.

Please **select YES/NO** as appropriate

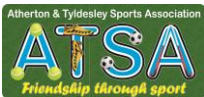
- Permission is given to be photographed for display in school: YES/NO
- Permission is given to be photographed for the school website: YES/NO
- Permission is given to be photographed for the class Twitter account: YES/NO
- Permission is given to be photographed for press releases for school events (Leigh Reporter/Leigh Journal etc): YES/NO
- Permission is given to be photographed for *ATSA Facebook page (**Sports teams**): YES/NO
(images may be 'shared' by 3rd parties)

Signed: _____ (parent/carer)

Date: _____

Please return this form to your child's teacher by **Wednesday 20th July 2016**

*Atherton and Tyldesley Sports Association



'Never settle for less than your best'

'Never settle for less than your best'