Online Safety Policy

Introduction

National guidance suggests that it is essential for schools to take a leading role in Online Safety. Becta in its "Safeguarding Children in a Digital World" suggested:

> *"That schools support parents/carers in understanding the issues and risks associated with children's use of digital technologies.*

The Byron Review "Safer Children in a Digital World" stressed the role of schools:

> *"One of the strongest messages I have received during my Review was about the role that schools and other services for children and families have to play in equipping children and their parents to stay safe online. To empower children and raise the skills of parents, I make recommendations to Government in the following areas: delivering Online Safety through the curriculum, providing teachers and the wider children's workforce with the skills and knowledge they need, reaching children and families through Extended Schools and taking steps to ensure that Ofsted holds the system to account on the quality of delivery in this area."*

Astley Park School takes its responsibility towards ICT, Online Safety and the education of all very seriously. The development and expansion of the use of ICT, and particularly of the internet, has transformed learning in schools in recent years. Children and young people will need to develop high level ICT skills, not only to maximise their potential use as a learning tool, but also to prepare themselves as lifelong learners and for future employment. There is a large body of evidence that recognises the benefits that ICT can bring to teaching and learning. Schools have made a significant investment both financially and physically to ensure these technologies are available to all learners. The benefits are perceived to "outweigh the risks." However, schools must, through their Online Safety policy, ensure that they meet their statutory obligations to ensure that children and young people are safe and are protected from potential harm, both within and outside school. The policy will also form part of the school's protection from legal challenge, relating to the use of ICT.

Schools are expected to evaluate their level of Online Safety in the Ofsted Self Evaluation Form (SEF) and will be subject to an increased level of scrutiny by Ofsted Inspectors during school inspections. Many schools are opting to gain recognition for the quality of their Online Safety provision through 360 Degree Safe (provided by SWGFL). This is something that Astley Park School is currently working towards. The 360 Degree Safe self-review tool contains a number of aspects which link into the school's Online Safety policies and provision.

Background / Rationale

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school.

The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and pupils learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe internet access at all times.

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 schools are bound. A school Online Safety policy should help to ensure safe and appropriate use. The development and implementation of such a strategy should involve all the stakeholders in a child's education from the headteacher and governors to the senior leaders and classroom teachers, support staff, parents, members of the community and the students / pupils themselves.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil achievement.

However, the use of these new technologies can put young people at risk within and outside the school. 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
- Online-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 it is essential that this Online Safety policy is used in conjunction with other school policies (e.g. Behaviour, Anti-Bullying and Child Protection policies).

Any incident of Online Safety, within school or which takes place beyond school, should be dealt with immediately by the member of staff that is made aware. The DSL, Behaviour for Learning Manager, Head or Deputy should be informed and will make the judgement as to whether the parents/carers should be contacted. Staff will complete the relevant CPOMS log to reflect the nature of the incident.

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build pupils' 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.

Schedule for Development / Monitoring / Review

This Online Safety policy was approved by the *Governing Body / Governors Sub Committee on:*	
The implementation of this Online Safety policy will be monitored by the:	LMT
Monitoring will take place at regular intervals:	*Once a year*
The *Governing Body / Governors Sub Committee* will receive a report on the implementation of the Online Safety policy generated by the monitoring group (which will include anonymous details of Online Safety incidents) at regular intervals:	*Once a year*
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 Online Safety or incidents that have taken place. The next anticipated review date will be:	January 2019
Should serious Online Safety incidents take place, the following external persons / agencies should be informed:	*Headteacher, DSL, LA Safeguarding Officer, Police Commissioner's Office*

The school will monitor the impact of the policy using:

- *Logs of reported incidents*
- *Internal monitoring data for network activity*
- *Surveys / questionnaires of*
  - *Students / pupils (e.g. Ofsted survey / CEOP ThinkUknow surveys)*
  - *Parents / carers*
  - *Staff*

Roles and Responsibilities

The school has implemented an Online Safety Group who meet regularly. The following section outlines the roles and responsibilities for Online 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. This will be carried out by the Governors upon receiving regular information about Online Safety incidents and monitoring reports. Governors are also required to sign the Acceptable Use Policy.

Headteacher and Senior Leaders:

The Headteacher and members of the Senior Leadership Team are responsible for ensuring the safety (including Online Safety) of members of the school community. The Leadership team are also required to sign the Acceptable Use Policy.

The Headteacher and members of the Leadership Management Team should be aware of the procedures to be followed in the event of a serious Online Safety allegation being made against a member of staff.

ICT Manager / Third Party Technical support staff:

The ICT Manager, Third Party ICT Technician for ensuring:

That the school's ICT infrastructure is secure and is not open to misuse or malicious attack.

That the school meets the Online Safety technical requirements outlined in the Technical Security Policy and Acceptable Usage Policy and any relevant Local Authority Online Safety Policy and guidance.

That users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed. (For further information on Password requirements please refer to school Technical Security Policy)

The Headteacher / ICT Manager is responsible for ensuring that the Online Safety Policy is followed and that all members of the Astley Park Community are safe.

They are required to carry out sanctions and requests for low level contravention of the policy.

They are required to carry out spot checks on software and hardware if deemed appropriate or if a concern is raised. This may include requesting to see staff laptops, USB/hard drives and personal areas on the school network.

Online Safety Subject Lead / Teaching and Support Staff (this may also include Ancillary staff):

Are responsible for ensuring that:

They have an up to date awareness of Online Safety matters and of the current school Online Safety policy and practices.

They have read, understood and signed the Astley Park Staff Acceptable Use Policy.

They report any suspected misuse or problem to the Headteacher or ICT Manager, or in their absence a member of the Leadership Team.

Digital communications with students / pupils (email / Virtual Learning Environment (VLE) / voice) should be on a professional level and only carried out using official school systems.

Online Safety issues are embedded in all aspects of the curriculum and other school activities.

Pupils understand and follow the school Online Safety policy.

Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.

They monitor Online Safety, Computing & ICT activity in lessons, extra-curricular and extended school activities.

They are aware of Online Safety issues related to the use of mobile phones, iPads, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these mobile devices.

In lessons where internet use is pre-planned pupils 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.

They fill in the appropriate log (CPOMS) for any pupil incident regarding the ICT / Online Safety policy being contravened.

Designated Senior Lead (DSL) for Safeguarding

Is trained in Online 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.
- Online-bullying.

(NB. it is important to emphasise that these are child protection issues, not technical issues, simply which the technology provides additional means for child protection issues to develop)

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 school will therefore take every opportunity to help parents understand these issues through Parents Evenings, Newsletters, Letters, Training Days, Website / Social Media and information about National / Local Online Safety campaigns and literature.

Policy Statements

Education – Pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in Online Safety is therefore an essential part of Astley Park's Online Safety provision. Children and young people need the help and support of the school to recognise and avoid Online Safety risks and build their resilience.

Online Safety education will be provided in the following ways

- A planned Online Safety Curriculum is in place and a focus in all areas of the curriculum this will cover both the use of ICT and new technologies in school and outside school
- KS3/4 Digital Leaders (Pupils) will promote Online Safety within classes
- Key Online Safety messages are reinforced as part of a planned programme of assemblies and tutorial / pastoral activities, including Safer Internet Day.
- Pupils 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
- Pupils are helped to understand the need for the Pupil AUP and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school
- Pupils are 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 posted in all rooms
- Staff should act as good role models in their use of ICT, the internet and mobile devices
- Pupils have access to our Whisper service. Whisper is our school's confidential system for reporting problems at school or at home. Pupils can choose whether to send the report anonymously or not. We have a dedicated page on our website for the Whisper service and it is also available for parent and carers to use too.

Education – Parents / Carers

Many parents and carers have only a limited understanding of Online 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 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. "There is a generational digital divide". (Byron Report).

Astley Park will therefore seek to provide information and awareness to parents and carers through:

- Parent's Evenings
- Newsletters / Website / Social Media
- Sharing Learning Days
- Family Support Co-ordinator / ICT Manager

Education - Extended Schools

Astley park is keen to ensure the safety of the whole school community and will offer family learning courses in ICT, Media Literacy and Online Safety so that parents and children can together gain a better understanding of these issues. Messages to the public around Online Safety should also be targeted towards grandparents and other relatives as well as parents. 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.

Education & Training – Staff

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

A planned programme of formal Online Safety training will be made available to staff. An audit of the Online Safety training needs of all staff will be carried out regularly. It is expected that some staff will identify Online Safety as a training need within the performance management process.
All new staff should receive Online Safety training as part of their induction programme, ensuring that they fully understand the school Online Safety policy and Acceptable Use Policies.

Training – Governors

Governors take part in Online Safety training / awareness sessions, with particular importance for those who are members of any sub committee / group involved in ICT / Online Safety / Health and Safety / Safeguarding. 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 school training / information sessions for staff or parents.

Technical – infrastructure / equipment, filtering and monitoring

Astley Park will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented.

- School ICT systems will be managed in ways that ensure that the school meets the Online Safety technical requirements outlined.
- There will be regular reviews and audits of the safety and security of school ICT systems.
- Servers, wireless systems and cabling must be securely located and physical access restricted.
- All users will have clearly defined access rights to school ICT systems.
- The "master / administrator" passwords for the school ICT system, used by the ICT Manager (or other person) must also be available to the Headteacher and/or SBM 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 school does not buy into Devolved filtering and for that reason all filtering is driven by the Local Authority guidelines using BTLS Lightspeed Filtering Service.

- School ICT Manager will regularly monitor and record the activity of users on the school ICT systems.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc from accidental or malicious attempts which might threaten the security of the school systems and data.
- The school infrastructure and individual workstations are protected by up to date virus software.
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.
- Photographs of pupils should NEVER be taken off site, whether encrypted or not.

Curriculum

Online Safety can be a focus in all areas of the curriculum and staff should reinforce Online Safety messages in the use of ICT across the curriculum.

- In lessons where internet use is pre-planned, it is best practice that students / pupils 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 pupils are allowed to freely search the internet, e.g. 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 (e.g. racism, drugs, and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the ICT Manager and in some cases the Local Authority 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.
- Pupils should be taught in all lessons to be critically aware of the materials / content they access online and be guided to validate the accuracy of information
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

Use of digital and video images - Photographic, Video

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupil's instant use of images that they have recorded themselves or downloaded from the internet. However, staff and pupils 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. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees. The school 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 pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In

particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.

- Staff are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the internet – website/school social media pages, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website, school social media pages or blog.
- Pupils' full names will never be shown with a photograph, this includes in and around school, the school website, school social media pages and any published materials.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website or school social media pages.
- Pupil's work can only be published with the permission of the pupil and parents or carers.

Data Protection

Astley Park's named Data Officer is Kieran Welsh (Headteacher).

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

Following a number of "high profile" losses of personal data by public organisations, schools are likely to be subject to greater scrutiny in their care and use of personal data. Astley Park follows Local Authority and National Guidance when dealing with data.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.

When personal data is stored on any portable computer system, USB pen drive or any other removable media:

- The data must be encrypted and password protected
- The device must be password protected and issued by the school (many USB pen drives and other removable media devices cannot be password protected). Personal USB pen drives or removable media devices ARE NOT ALLOWED in school.
- The device must offer approved virus and malware checking software
- Each member of staff is allocated 1TB (1000gb) of OneDrive cloud storage which must be utilised instead of USB pen drives/external drives. OneDrive is part of the Office 365 subscription of each member of staff and is a secure method to store files (only upload files keeping within school policies). This method also reduces the risk of losing data / unauthorised access / virus / malware and ransomware attacks.
- In the event of an external visitor needing to use a USB Pen Drive/removable media to deliver training this must be authorised by the Headteacher / ICT Manager in advance of the training session.

Communications

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

	Staff & other adults				Students / Pupils			
Communication Technologies	Allowed /locked away in locker/staff room	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed/locked away in locker	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school	x	x			x			
Use of mobile phones in lessons				x				x
Use of mobile phones in social time		x						x
Taking photos on mobile phones or other camera devices				x				x
Use of other mobile devices e.g. iPads, PDAs			x	x				x
Use of personal email addresses in school, or on school network				x				x
Use of school 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				x

*official school social networking pages only

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

- The official school email service may be regarded as safe and secure and is monitored. Staff and students / pupils should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access).
- Users need to be aware that email communications may be monitored
- Users must immediately report, to the Headteacher or ICT Manager – in accordance with the school policy, 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 / pupils or parents / carers (email, chat, VLE etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or public chat / social networking programmes must not be used for these communications.
- Pupils are 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 school website and only official email addresses should be used to identify members of staff.

Unsuitable / inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other ICT systems. Other activities e.g. Online-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities. The school believes that the activities referred to in the following section would be inappropriate in a school context and those users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems.

Use of Mobile Phones

- Mobile Phones are allowed in school during working hours.
- However they are only permitted to be switched on in the staffroom during break or lunchtime.
- In exceptional cases mobile phones are allowed to be used outside of these times, but only with prior permission of the Headteacher.
- Staff should list the school telephone number 01257 262227 as their emergency contact number, should they need to be contacted during the school day.
- Visit leaders and Deputy leaders are allowed to take a mobile phone out on Educational Visits this should be included within the visit risk assessment.
- Named members of staff in school may need to use a mobile phone/iPad as part of their role in school and will not use these for personal reasons during the school day.

- If a member of staff is found to have their phone switched on or to be using their mobile phone anywhere other than in the designated area or without prior permission from the Headteacher then they will be in breach of school policy and disciplinary action will be taken.

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, e.g. 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 school or brings the school into disrepute				x	
Using school systems to run a private business					x	
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by SWGfL and / or the school					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 (e.g. 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	
Online gaming (educational)			x			
Online gaming (non educational)					x	

Online gambling				x	
Personal Online shopping / commerce				x	
Use of social networking sites (*official school social media pages only)			x*	x	
Use of video broadcasting e.g. Youtube			x	x	

Staff Incidents:	Refer to line manager	Refer to Headteacher	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 / social networking sites / instant messaging / personal email		x				x	x	x
Unauthorised downloading or uploading of files		x				x	x	x
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		x				x	x	x
Careless use of personal data e.g. holding or transferring data in an insecure manner		x				x	x	x
Deliberate actions to breach data protection or network security rules		x				x	x	x
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		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
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils		x				x	x	x
Actions which could compromise the staff member's professional standing		x					x	x
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		x				x	x	x
Using proxy sites or other means to subvert the school's filtering system		x				x	x	x
Accidentally accessing offensive or pornographic material and failing to report the incident		x				x	x	x

Deliberately accessing or trying to access offensive or pornographic material		x					x	x
Breaching copyright or licensing regulations		x				x	x	x
Continued infringements of the above, following previous warnings or sanctions		x					x	x

Appendix

Staff Online Safety Policy please refer to the LCC Social Media Policy
http://www3.lancashire.gov.uk/corporate/web/viewdoc.asp?id=129797

Date policy approved by Governing Body Curriculum & Policy Committee: 16.05.18

Signed Chair of Curriculum & Policy Committee: _____

Mr M Maher

Signed Chair of Governing Body: _____

Mrs W Blundell

Policy Review Date: Spring Term 2019