Atelier —21—

a revolutionary response to school

E-Safety Policy

Policy to be read in conjunction with:

- DfE – Keeping Children Safe in Education (KCSIE) 2021
- HM Government - Working Together to Safeguard Children 2020
- DfE - The Prevent Duty June 2015
- The use of Social Media for online radicalisation (July 2015) DfE – How social media is used to encourage travel to Syria and Iraq
- Safeguarding and Child Protection Policy
- Bring Your Own Device Policy
- Anti-Bullying policy
- Personal, Social, Health and Economic Education (PSHEE) Policy
- Social, Moral, Spiritual and Cultural (SMSC) Policy
- Behaviour Management Policy
- Health and Safety Policy
- Mobile phone use Policy
- Equal Opportunities Policy
- Data Protection Policy
- Computing Policy
- Curriculum Policies and Schemes of Work

Rationale

The curriculum at Atelier 21 is based on the principles of independent learning, as a result, pupils use a variety of resources when carrying out research. The school is aware of its responsibility to keep pupils safe while they are using digital technology in school and in their daily lives. The school has appropriate, monitored, filters in place to protect pupils but we recognise that it is impossible to totally eliminate risk. We aim to provide pupils with the knowledge and skills that will protect them when working online, give them the confidence to report any issues to a trusted adult and make them resilient so that they can overcome any potential issues.

The school is committed to acting in the best interests of children. The school's procedures for dealing with or referring concerns about children in need or risk are in accordance with locally agreed inter-agency procedures which can be found within the Safeguarding Policy.

The school has a listening culture and pupils are encouraged to discuss any anxieties or concerns with staff.

The school takes internet safety very seriously. All allegations of misuse of equipment will be investigated and the school will work with external agencies, including the police, where necessary.

If an allegation against a member of staff is upheld the school will report the matter to the Disclosure and Barring Service and the Teacher regulation Agency (TRA).

Some of the dangers that pupils may face when working online are:

- access to illegal, harmful or inappropriate images or other content
- unauthorised access to/ loss of or sharing of personal information
- the risk of being groomed
- the sharing/distribution of personal images without their consent
- inappropriate communication with others
- cyber- bullying
- sexting
- radicalisation
- peer pressure
- suicidal thoughts or the promotion of eating disorders or self-harming
- access to unsuitable video/internet games
- online gambling
- an inability to evaluate the quality, accuracy and relevance of information on the internet
- plagiarism and copyright infringement or Illegal downloading of music or video files
- the potential for excessive use, including all night gaming, which may impact on the social and emotional development and learning of pupils

Scope of the policy

The policy applies to all members of the school community, staff, pupils, volunteers, parents/carers and visitors.

The school expects pupils and staff to apply the same high standards of online safety in and outside of school. The school will impose disciplinary penalties for any inappropriate behaviour, this includes incidents of cyber bullying or other e-safety related matters. The school will deal with any incidents within the scope of this policy and the Safeguarding and Child Protection, Behaviour Management, and Anti-bullying Policies. The school will inform parents of any incidents of inappropriate e-safety behaviour which take place in or outside school.

The school will monitor the effectiveness of this policy using logs of reported incidents and unacceptable behaviour. The policy will be reviewed annually.

Aims

- to ensure that pupils are safe when online
- to inform pupils, staff and parents
- to ensure that pupils, staff and parents are aware of their responsibilities in this area
- to ensure that the school deals with any issues in a prompt and effective manner

Roles and Responsibilities

The Proprietor

- is responsible for ensuring the health and safety, including e-safety, of all members of the school community
- will ensure that the school has appropriate safeguards in place to protect pupils and staff while they are working online
- is responsible for ensuring that all staff receive appropriate training to help them carry out their roles
- will ensure that there is a system in place to monitor and support staff who carry out an E-safety role
- will ensure that all incidents are recorded in the e-safety log
- will deal with all incidents in accordance with school policies
- will monitor and evaluate the incident log, liaise with staff, parents and other agencies and review the school's systems where necessary
- will apply the Safeguarding/Disciplinary Policy when dealing with an allegation made about a member of staff
- will ensure that all staff read the policy and are familiar with the procedures for reporting incidents.

The Designated Safeguarding Lead (DSL) and Deputy Designated Safeguarding Lead (DDSL)

- will be trained in e-safety issues and know how to deal with any incidents that occur, including referrals to external agencies
- will ensure that the curriculum provides pupils with information and guidance on e-safety matters
- will provide support for pupils and staff
- will report incidents to the local authority safeguarding team where necessary.

Staff

- will ensure that they read all relevant policies and have a secure understanding of e-safety matters
- will ensure that they have read, understood and signed the Staff Acceptable Use Agreement
- will ensure that they report any suspected misuse to the proprietor for investigation
- will ensure that all digital communications with pupils and parents are only carried out using official school systems/email
- will be aware that school email accounts may be monitored
- will check that emails sent on the school account to external organisations are appropriate and authorised by the proprietor/senior member of staff before sending
- will ensure that e-safety considerations are embedded in all aspects of the curriculum and other school activities
- will not take personal mobile phones or tablets/laptops into classrooms without the prior agreement of the proprietor
- will ensure that pupils understand and follow the E-safety Policy and the Acceptable Use Agreement
- will monitor ICT activity in lessons, extra –curricular and other school activities
- will ensure that they are aware of e-safety issues related to the use of mobile phones, cameras and other devices and implement current school policies with regard to the use of these devices
- will support pupils using the internet, guide pupils to appropriate sites and understand and apply the school's systems for dealing with any unsuitable material that is found

- will provide a calm and approachable listening ear and deal with any incidents by following the school E-safety Policy, Safeguarding Policy or any other relevant policy.
- Will ensure that any personal laptops are installed with Impero software (more information within the BYOD policy)

Pupils

- are responsible for using school ICT systems in accordance with the acceptable use policy
- will understand the importance of reporting any incidents of abuse, misuse or inappropriate usage and know how to do so
- will understand the importance of adopting safe e-safety practices when using digital technologies outside of school
- will ensure that any personal laptops are installed with Impero software (more information within the BYOD policy)

Parents/Carers

Parents/carers play a crucial role in ensuring that their children use digital technologies safely. Research shows that many parents do not fully understand the risks to children and may feel that 'it wouldn't happen to my child'. The school will help parents understand the issues through the use of workshops, newsletters, email and information about national/local e-safety campaigns. Parents/carers are advised to always have parental control settings on home devices, consider the age at which pupils should have social media accounts and/or mobile phones and monitor their children's accounts. Parents and carers must:

- sign the Pupil Acceptable Use Agreement
- ensure that pupils do not use the internet/social media sites and other forms of digital communication in an inappropriate or defamatory way
- sign the Impero Monitoring and Filtering Agreement for those wishing their children to use personal laptops within the school

Managing Information Systems

- staff must take responsibility for network use and the use of school resources, failure to comply with the school Acceptable Use Agreement may be grounds for dismissal
- the school will ensure that virus protection is installed and current on all school owned devices
- the school will ensure that appropriate filters are in place and that they are monitored
- the school will ensure that the server operating system is secured and kept up-to-date
- staff may not link personal devices to the school system, e.g. USB drives, they may not use unapproved software on school devices or attach such software to emails
- a secure user name/password system has been established and applies to all school systems including email, all adults are responsible for the security of their user names and passwords and must not allow others to access the system using their log in details, they must report any breach of security to the proprietor
- passwords must be changed every 90 days, passwords must be a minimum of eight characters long and must include upper case, lower case, a number and a special character
- staff and pupils must use logins and passwords to access the school system, these will be changed regularly and should not be shared with others
- no user should access other user's files without permission
- access to personal data is securely controlled in- line with the Data Protection Policy

Emailing Personal, Sensitive, Confidential or Classified Information

Email is not a secure means of transmitting information so consider if the information could be transmitted by other secure means before emailing it. The use of any internet-based web mail service, other than that used by the school, for sending emails containing sensitive information is not permitted.

If email to external email addresses must be used to send confidential information staff must:

- obtain consent from the proprietor
- exercise caution when sending the email
- verify the details, including an accurate email address, of any intended recipient
- verify, by phoning, the intended recipient before sending any information, where possible look up phone numbers do not use details present on any email request
- do not send the email if you cannot verify the recipient's details
- do not copy or forward the email to other recipients
- send the information as an encrypted document attached to the email
- provide the encryption key in a separate document
- do not identify the information in the subject line
- request confirmation of safe receipt

Use of Digital Images

Pupils, staff and parents are made aware of the benefits and risks of sharing images on the internet. Pupils will understand that content remains on the internet forever, may be shared thousands of times and may cause harm or embarrassment to individuals in the short or longer term.

When using digital images staff:

- will Inform pupils of the risks associated with the taking, use, sharing, publication and distribution of images
- will ensure that parents have given consent for images of their child to be taken or published on the school's website
- may take digital images to support educational aims but must follow school policies with respect to the sharing, publication and distribution of images
- may only record image on school equipment and with the permission of the proprietor
- must ensure that when taking images pupils are appropriately dressed and are not participating in activities which could bring the school or individuals into disrepute
- will ensure that images published on the school website are selected carefully and comply with good practice guidance on the use of such images
- will ensure that pupils full names are not used anywhere on a website or blog and not in association with a photograph
- will not view any images or material which are the subject of a bullying or a safeguarding incident

Pupils must not:

- Take, use, share, view, distribute or publish images of others with or without their consent

Managing Skype/Video Conferencing etc.

There are many benefits to this type of communication, but appropriate safeguards need to be in place. Teachers must check who is participating in the call as a guest without a camera will not be visible.

- all equipment must be switched off when not in use and not set to auto answer
- teachers must know how to use the technology and how to end the call if any participant becomes unhappy with the content
- pupils will ask permission from the teacher before making or answering a skype call
- parental consent is required before pupils participate in video conferencing/skype or Youtube programme making. Written permission will be sought for pupils to create content which will be used on social media sites
- if teachers are working from home and delivering lessons via technology they must ensure that the system is secure and that they check the walls behind their screen and the area around it to ensure that no inappropriate or personal images can be seen by children
- if teachers are working remotely with pupils they must be alert to any evidence of safeguarding concerns or disclosures, if there is a concern or disclosure these should be recorded and discussed with the DSL/DDSL or directly with West Sussex Safeguarding Children Partnership.

Data protection

Staff must ensure that they:

- keep personal/school data safe minimising the risk of its loss or misuse
- use personal data only on secure password protected devices
- ensure that they are properly logged off at the end of any session
- transfer data using encrypted and secure password protected devices
- do not use USB sticks to store data
- delete all data once its use is complete

Assessing Risk

The school recognises that it is not possible to guard against every undesirable situation. Pupils are supervised while using devices and all pupils are taught how to stay safe when online. The school takes all reasonable precautions to ensure that users only access appropriate material but because of the global and connected nature of internet content it is not possible to guarantee that pupils will never access unsuitable material. The school cannot accept liability for the materials accessed or any consequences resulting from internet use. The school will audit ICT use and the E-Safety Policy will be reviewed on an annual basis or when guidance or legislation changes. The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence and breaches will be reported to the police.

Unsuitable/Inappropriate Activities

Users will not visit internet sites, make, post, download, upload, data transfer, communicate or pass on material, remarks, proposals or comments that contain or relate to:

- images of child sexual abuse

- promotion or conduct of illegal acts under the child protection, obscenity, computer misuse and fraud legislation
- adult material that breaches the Obscene Publications Act in the UK
- racist material
- pornography
- promotion of discrimination
- promotion of racist or religious hatred
- materials with political bias
- threatening behaviour, including the promotion of physical violence or mental harm
- any other information which may be offensive to colleagues, breaches the ethos of the school or brings the school into disrepute
- online gaming
- online gambling
- online shopping
- file sharing
- use of social networking or broadcasting sites

Users will not;

- upload, download or transmit commercial software or any copyrighted materials belonging to third parties without the necessary licensing permissions
- reveal or publicise confidential or proprietary (financial, personal, databases, computer/network access codes and passwords)
- create or propagate computer viruses or other harmful files
- use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards used by the school

Responding to Incidents

E-safety risks can be experienced unintentionally or deliberately by people acting inappropriately or illegally. Teachers' observation of pupils' behaviour is an important strategy in identifying concerns about pupils and developing trust so that concerns are reported. Staff are responsible for creating a culture of safeguarding in which any potential concerns are reported to the proprietor/DSL. Incidents of concern include, 'jokes', 'banter' or inappropriate actions.

Teachers/staff must not view any images of children or young people when dealing with incidents of online abuse or bullying, the device should be handed over to the police and /or children's services as required.

Where there is cause for concern or a fear that illegal activity is taking place the school will contact the West Sussex Safeguarding Children Partnership, Integrated Front Door and /or the police. Evidence of online radicalisation will be dealt with under the Prevent Strategy. Where the incident involves misuse of equipment by a child the incident will be dealt with under the appropriate policy.

Complaints about E-safety will be dealt with under the Complaints Policy, Safeguarding and Child Protection Policy, Anti-Bullying, or Behaviour Management Policy. All complaints and /or incidents are recorded by the school. The school is aware of the importance of confidentiality when dealing with complaints about pupils or staff.

Policy Requirements

- all staff will read and sign the Acceptable Use Agreement
- parents and pupils, where appropriate, will read and sign the Acceptable Use Agreement for pupil access
- visitors who require access to the school's system will sign an Acceptable Use Agreement.
- most visitors, including parents, will be asked to switch off mobile phones and not use them in school, the exceptions are inspectors and a small number of other professionals
- the school will make digital recordings of any concerts, presentations or special events, taking account of the permissions given by parents. Parents will be provided with free copies of these recordings
- parents are informed that pupils have access to the internet
- parents and pupils, where appropriate, will read and sign the Impero Monitoring and Filtering Agreement for use of personal laptops within school
- all staff, where appropriate, will read and sign the Impero Monitoring and Filtering Agreement for use of personal laptops within school

Cyber Bullying

Cyber bullying is defined as the use of digital technology, particularly mobile phones and the internet, to deliberately hurt or upset others. When children are the target of online bullying they often feel very isolated particularly if the adults around them do not understand the impact of this type of bullying. It is essential that pupils, staff and parents understand the impact of cyber bullying, how it affects children and how to respond and combat misuse. The creation of a caring school community within which pupils develop self-confidence and resilience and learn to respect others is an important strategy in combatting all types of bullying.

When bullying that happens outside of school is reported the school will investigate. The perpetrator will be asked to delete all offensive comments or materials, a service provider will be contacted and asked to remove content if the perpetrator cannot do so. Parents will be informed and the incident may result in short term or permanent exclusion. The police or LA safeguarding team may be informed if the school suspects a criminal offence has taken place.

Teaching and Learning

Internet use is part of the curriculum and is an important tool for learning, the school provides pupils with access to the internet as part of their learning experience. The internet and digital technologies are part of everyday life and are used by pupils in all aspects of their lives so it is important that they are aware of the benefits this can bring and know how to protect themselves, stay safe and report any inappropriate usage. The benefits of using the internet include:

- access to international resources including museums and galleries
- educational and cultural exchanges between people
- access to 'experts' for pupils and staff
- professional development for staff
- access to learning wherever and whenever it is convenient

We aim to produce resilient learners with a strong sense of personal and collective responsibility, we encourage all pupils to work together to ensure that everyone is safe and to report anything which is causing them concern or anxiety.

Pupils with Special Educational Needs (SEND)

Pupils identified as having special educational needs and disabilities or those requiring additional support will receive teaching which is appropriate to their needs. They will be supervised when accessing information, if required, and they will be helped to access resources which are appropriate for their needs and ability. The school will attempt to provide appropriate resources for all users.

Evaluating Internet Content

There is a plethora of information available on the internet but not all information is accurate or reliable. Identifying inaccurate information, comparing sources and checking for reliability is an important life skill. Critical thinking and evaluative skills are taught during English lessons, at an appropriate level, and are reinforced during self-directed learning and collaborative work. Pupils are taught to compare sources, look at the origin of sources and check for bias. They will understand the difference between fact and opinion and will begin to identify where information may be misleading or dangerous. Pupils will apply their skills in all curriculum areas and though discussions and collaborations with others.

Resources

- The UK Safer Internet Centre (https://www.saferinternet.org.uk/about)
- CEOP’s Think know website (www.thinkuknow.co.uk) (Child Exploitation and Online protection Centre)
- National Education Network (NEN)

Document Control Information			
Author	Hayley Peacock	**Status**	Approved
Version	1.3	**Date**	3/11/2021
Approved by	Hayley Peacock	**Signed**	HPeacock .
Approved Date	3/11/2021	**Review Date**	3/11/2022
Location	https://atelier21schools.co.uk/parents/#Policies		

Document Review			
Version	**Amendment**	**By**	**Date**
1.0	Initial Release	H Peacock	January 2020
1.1	minor formatting changes	D Hearn	15/06/2020
1.2	Change to document dates	Danni Hayes	13/05/2021
1.3	Addition to add Impero, and update safeguarding details	Danni Hayes	3/11/2021

Appendix 1 - Atelier 21 Pupil Acceptable Use Agreement

These rules will help us to keep everyone in our school safe.

- I will only use ICT in school for educational/approved purposes
- I will only use my school email address when emailing in school
- I will only open email attachments from people I know or those my teacher has approved
- I will not share my passwords with others
- I will only open or delete my own files
- I will make sure all my contacts with others are responsible, polite and kind
- I will not deliberately look for, save or send anything which is unpleasant or upsetting. If I accidently find anything like this I will tell my teacher immediately
- I will not give out my personal details (my name, address or phone number). I will not arrange to meet anyone I meet online
- I will behave responsibly when working online because I know the rules are to keep me safe
- I will not take my mobile phone into lessons
- I know my use of ICT can be checked and I know the school may contact my parents if staff are worried about my safety

………

Pupil Acceptable Use – Parent/ Carer/Pupil Agreement

We have read the safety rules and ……………………………………….. (child's name) agrees that he/she will follow the e-safety rules and support the safe use of digital technologies at Atelier 21.

Signature ……………………………………………………….

Parent Name		Pupil's Name	
Signed		Date	

Appendix 2 - Atelier 21 Staff/ Visitor Acceptable Use Agreement

ICT, including data, and the related technologies such as email, the internet and mobile devices are an integral part of life in school. This agreement aims to ensure that all staff are aware of their professional responsibilities when using any form of ICT. This applies to ICT use in school, the use of school ICT systems and equipment outside of school, the use of personal ICT equipment in school or in situations related to employment in school. All staff and visitors are expected to read and sign this agreement and comply with its content. Any concerns should be discussed with the proprietor.

- I will only use the school's email, internet and any related technologies for professional purposes deemed appropriate by the proprietor
- I will comply with ICT system security and I will not disclose any passwords provided to me by the school
- I will not give out my personal details such as personal email address or mobile phone number to parents or pupils
- I will only use the approved, secure email system for any school business
- I will ensure that any personal data is kept securely and is used appropriately, I understand that any personal data taken off site must be encrypted
- I will not install any hardware or software without permission and appropriate licenses
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory
- Images of pupils and /or staff will only be taken using school equipment and with the required permissions. Images will not be distributed outside of the school network without the permission of the proprietor and parent or carer
- I understand that my internet usage and my use of other related technologies can be monitored and logged and can be made available to the police or other external agencies
- I will support the school's approach to online safety and not deliberately upload or add any images, video , sounds or text that could offend or upset any member of the online community or bring the school into disrepute
- I will respect copyright and intellectual property rights
- I will ensure that my personal and professional online activity will not bring my professional role into disrepute
- I will not take personal mobile phones or devices into classrooms or outdoor areas without the permission of the proprietor
- I will support and promote the school's E-safety, Safeguarding, Data Protection, Anti-Bullying and Behaviour Policies and help pupils to be safe and responsible in their use of ICT and other related technologies
- I understand that this agreement forms part of my terms and conditions of employment (staff)
- I understand that if I fail to comply with the Acceptable Use Agreement I could be subject to disciplinary action
- ………

Staff/Visitor Acceptable Use Agreement

I have read and understood the information and agree to use the school's ICT systems, both in and out of school, and my own devices. I agree to comply with the agreement and support the safe and secure use of ICT throughout the school.

Name	
Job Title	
Signed/Date	