



Cupernham
Junior School

ONLINE SAFETY AND ACCEPTABLE USE OF TECHNOLOGY POLICY

Policy Published:	SEPTEMBER 2026
Policy Amendments:	
Full Governing Body Approval:	SEPTEMBER 2026
Review Date:	SEPTEMBER 2027

This policy was updated in September 2026 and has undergone an Equalities Impact Assessment in line with the requirements of the Public Sector Equality Duty.

CUPERNHAM JUNIOR SCHOOL IS A SMARTPHONE FREE AND SMART-DEVICE FREE SCHOOL

SCOPE OF THE ONLINE SAFETY POLICY

This Online Safety Policy outlines the commitment of Cupernham Junior School to safeguard members of our school community online in accordance with statutory guidance and best practice.

This Online Safety Policy applies to all members of the school community (including staff, learners, governors, volunteers, parents and carers, visitors, community users) who have access to and are users of school digital systems, both in and out of the school. It also applies to the use of personal digital technology on the school site (where allowed).

Cupernham Junior School will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that take place out of school.

This Online Safety Policy has been developed by consultation with:

- Senior leaders
- Designated safeguarding lead (DSL) and Safeguarding team
- Staff – including teachers/support staff/site team
- Governors

The DfE guidance “Keeping Children Safe in Education” states:

“Online safety and the school or college’s approach to it should be reflected in the child protection policy”. School have made the decision to reference this within the Child Protection Policy and to have a separate Online Safety (and Acceptable Use of Technology) Policy as well.

The school Online Safety Policy:

- sets expectations for the safe and responsible use of digital technologies for learning, administration, and communication
- allocates responsibilities for the delivery of the policy
- is regularly reviewed in a collaborative manner, taking account of online safety incidents and changes/trends in technology and related behaviours
- establishes guidance for staff in how they should use digital technologies

responsibly, protecting themselves and the school and how they should use this understanding to help safeguard learners in the digital world

- describes how the school will help prepare learners to be safe and responsible users of online technologies
- establishes clear procedures to identify, report, respond to and record the misuse of digital technologies and online safety incidents, including external support mechanisms
- is supplemented by a series of related acceptable use agreements
- is made available to staff at induction and through normal communication channels via CPOMS, staff briefings and minutes, and is published on the school website

ONLINE SAFETY EDUCATION PROGRAMME

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- ❖ A planned online safety curriculum for all year groups matched against a nationally agreed framework - Education for a Connected Work Framework by UKCIS/DCMS and the SWGfL Project Evolve and taught through 8 lessons across the year
- ❖ Lessons are matched to need; are age-related and build on prior learning
- ❖ Lessons are context-relevant with agreed objectives leading to clear and evidenced outcomes
- ❖ Digital competency is planned and effectively threaded through the appropriate digital pillars in other curriculum areas e.g. PHSE; RSE; English etc.
- ❖ it incorporates/makes use of relevant national initiatives and opportunities e.g. Online Safety Day and Anti-Bullying Week
- ❖ the programme will be accessible to learners at different ages and abilities such as those with additional learning needs or those with English as an additional language.
- ❖ vulnerability is actively addressed as part of a personalised online safety curriculum e.g., for victims of abuse and SEND.
- ❖ staff should act as good role models in their use of digital technologies, online usage and through and mobile devices
- ❖ in lessons where online access use is pre-planned, it is best practice that learners 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 online searches
- ❖ where learners are allowed to freely search online, staff should be vigilant in supervising the learners and monitoring the content of the websites the young people visit
- ❖ the online safety education programme should be relevant and up to date to ensure the quality of learning and outcomes.

STAFF AND VOLUNTEERS

All staff will receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- ❖ the training will be an integral part of the school's annual safeguarding and data protection training for all staff
- ❖ all new staff will receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and acceptable use agreements. It includes explicit reference to classroom management, professional conduct, online reputation and the need to model positive online behaviours.
- ❖ the Online Safety Lead and Designated Safeguarding Lead (or other nominated person) will receive regular updates through attendance at external training events, (e.g. UKSIC / SWGfL / MAT / LA / other relevant organisations) and by reviewing guidance documents released by relevant organisations
- ❖ this Online Safety Policy and its updates will be presented to and discussed by staff
- ❖ the Designated Safeguarding Lead/Online Safety Lead (or other nominated person) will provide advice/guidance/training to individuals as required.

The school's Online Safety Lead is Mr Jack Wright.

GOVERNORS

Governors should take part in online safety training/awareness sessions. This may be offered in several ways such as:

- ❖ attendance at Governor meeting where safeguarding and online safety training takes place
- ❖ optional attendance at training provided by the local authority or other relevant organisation (e.g., SWGfL)
- ❖ participation in school training / information sessions for staff or parents

A higher level of training will be made available to (at least) the Safeguarding Governor. This will include:

- ❖ cyber-security training (at least at a basic level)
- ❖ training to allow the governor to understand the school's filtering and monitoring provision, in order that they can participate in the required checks and review.

FAMILIES

Parents and carers play an essential role in the education of their children and in the monitoring/regulation of the children's online behaviours. Technology and software is ever evolving and parents may underestimate how often children and young people come across potentially harmful and inappropriate material online and may be unsure about how to respond.

The school will seek to provide information and awareness to parents and carers through:

- ❖ regular communication, awareness-raising and engagement on online safety issues, curriculum activities and reporting routes
- ❖ the learners – who are encouraged to pass on to parents the online safety messages they have learned in lessons and by learners leading sessions at parent/carer evenings.
- ❖ letters, newsletters, website, learning platform,
- ❖ reference to the relevant web sites/publications, e.g. SWGfL; www.saferinternet.org.uk/; www.childnet.com/parents-and-carers
- ❖ sharing good practice with other schools in clusters and or the local authority/MAT

FILTERING & MONITORING

The school filtering and monitoring provision is agreed by senior leaders, governors and the IT Service Provider and is regularly reviewed (at least annually) and updated in response to changes in technology and patterns of online safety incidents/behaviours

Day to day management of filtering and monitoring systems requires the specialist knowledge of both safeguarding and IT staff to be effective. The DSL will have lead responsibility for safeguarding and online safety and the IT service provider will have technical responsibility

The filtering and monitoring provision are reviewed annually by senior leaders, the Designated Safeguarding Lead and a governor with the involvement of the IT Service Provider.

- ❖ checks on the filtering and monitoring system are carried out by the IT Service Provider with the involvement of a senior leader, the Designated Safeguarding Lead and a governor, in particular when a safeguarding risk is identified, there is a change in working practice, e.g. remote access or BYOD or new technology is introduced e.g. using SWGfL Test Filtering

FILTERING

- ❖ the school manages access to content across its systems for all users and on all devices using the school's internet provision - currently Schools Broadband. The filtering provided meets the standards defined in the DfE Filtering standards for schools and colleges and the guidance provided in the UK Safer Internet Centre Appropriate filtering.
- ❖ illegal content (e.g., child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation URL list and the police assessed list of unlawful terrorist content, produced on behalf of the Home Office. Content lists are regularly updated
- ❖ there are established and effective routes for users to report inappropriate content, recognising that no system can be 100% effective
- ❖ there is a clear process in place to deal with, and log, requests/approvals for filtering changes
- ❖ filtering logs are regularly reviewed and alert the Designated Safeguarding Lead to breaches of the filtering policy, which are then acted upon.
- ❖ the school has (if possible) provided enhanced/differentiated user-level filtering (allowing different filtering levels for different abilities/ages/stages and different groups of users: staff/learners, etc.)
- ❖ the school has a mobile phone policy of no mobile phone access for children during the school day. For safety, children's personal mobile devices are handed in and stored in a locked cupboard during the day
- ❖ access to content through non-browser services (e.g. apps and other mobile technologies) is managed in ways that are consistent with school policy and practice. If necessary, the school will seek advice from, and report issues to, the SWGfL Report Harmful Content site.

MONITORING

The school has monitoring systems in place to protect the school, systems and users:

- ❖ The school monitors all network use across all its devices and services.
- ❖ monitoring reports are urgently picked up, acted on and outcomes are recorded by the Designated Safeguarding Lead, all users are aware that the network (and devices) are monitored.
- ❖ There are effective protocols in place to report abuse/misuse. There is a clear process for prioritising response to alerts that require rapid safeguarding intervention.
- ❖ Management of serious safeguarding alerts is consistent with safeguarding policy and practice. The school follows the UK Safer Internet Centre Appropriate Monitoring guidance and protects users and school systems through the use of the appropriate blend of strategies informed by the school's risk assessment. These may include:

- ❖ physical monitoring (adult supervision in the classroom)
- ❖ internet use is logged, regularly monitored and reviewed
- ❖ filtering logs are regularly analysed and breaches are reported to senior leaders

TECHNICAL SECURITY

- ❖ The school technical systems will be managed in ways that ensure that the school meets recommended technical requirements
- ❖ responsibility for technical security resides with SLT who may delegate activities to identified roles
- ❖ all users have clearly defined access rights to school technical systems and devices. Details of the access rights available to groups of users will be recorded by the IT service provider and will be reviewed, at least annually, by the SLT/Safeguarding Team
- ❖ password policy and procedures are implemented. (consistent with guidance from the National Cyber Security Centre)
- ❖ the security of their username and password and must not allow other users to access the systems using their log on details
- ❖ all users have responsibility for the security of their username and password and must not allow other users to access the systems using their log on details.
- ❖ all school networks and system will be protected by secure passwords. Passwords must not be shared with anyone.
- ❖ the administrator passwords for school systems are kept in a secure place, e.g. school safe.
- ❖ there will be regular reviews and audits of the safety and security of school technical systems
- ❖ servers, wireless systems and cabling are securely located and physical access restricted
- ❖ appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems and devices from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by upto-date endpoint software.
- ❖ there are rigorous and verified back-up routines, including the keeping of network-separated (air-gapped) copies off-site or in the cloud,
- ❖ The School Business Manager is responsible for ensuring that all software purchased by and used by the school is adequately licenced and that the latest software updates (patches) are applied.
- ❖ an appropriate system is in place for users to report any actual/potential technical incident/security breach to the relevant person, as agreed)
- ❖ use of school devices out of school and by family members is regulated by an acceptable use statement that a user consents to when the device is allocated to them
- ❖ staff members are not permitted to install software on a school-owned device

- without the consent of the SLT/IT service provider
- ❖ removable media is not permitted unless approved by the SLT/IT service provider
- ❖ systems are in place to control and protect personal data and data is encrypted at rest and in transit.
- ❖ mobile device security and management procedures are in place
- ❖ guest users are provided with appropriate access to school systems based on an identified risk profile.

ACCEPTABLE USE

The school has defined what it regards as acceptable/unacceptable use and this is shown in the tables below.

The Online Safety Policy and acceptable use agreements define acceptable use at the school. The acceptable use agreements will be communicated/re-enforced through:

- ❖ staff induction
- ❖ communication with parents/carers
- ❖ built into education sessions
- ❖ school website

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not access online content (including apps, games, sites) to make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Any illegal activity for example: • Child sexual abuse imagery* • Child sexual abuse/exploitation/grooming • Terrorism • Encouraging or assisting suicide • Offences relating to sexual images i.e., revenge and extreme pornography • Incitement to and threats of violence • Hate crime • Public order offences - harassment and stalking • Drug-related offences • Weapons / firearms offences • Fraud and financial crime including money laundering					X
Users shall not undertake activities that might be classed as cyber-crime under the Computer Misuse Act (1990)	• Using another individual's username or ID and password to access data, a program, or parts of a system that the user is not authorised to access (even if the initial access is authorised) • Gaining unauthorised access to school networks, data and files, through the use of computers/devices • Creating or propagating computer viruses or other harmful files • Revealing or publicising confidential or proprietary information (e.g., financial / personal information, databases, computer / network access codes and passwords) • Disable/Impair/Disrupt network functionality through the use of computers/devices • Using penetration testing equipment (without relevant permission)					X
Users shall not undertake activities that are not illegal but are classed as unacceptable in school policies:	Accessing inappropriate material/activities online in a school setting including pornography, gambling, drugs. (Informed by the school's filtering practices and/or AUAs)				X	
	Promotion of any kind of discrimination				X	
	Using school systems to run a private business				X	

User actions	Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Using systems, applications, websites or other mechanisms that bypass the filtering/monitoring or other safeguards employed by the school				X	
Infringing copyright				X	
Unfair usage (downloading/uploading large files that hinders others in their use of the internet)				X	
Any other information which may be offensive to others or breaches the integrity of the ethos of the school or brings the school into disrepute				X	

	Staff and other adults				Learners		
	Not allowed	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times
Social Media			X breaktimes		X		
Online shopping				X admin and purchasing card holders	X		
Use of broadcasting (You tube, Tik Tok etc)				X as agreed by Head	X		
Mobile phones brought to school		X				X but locked away	
Mobile phones for learning		X but agreed with Head			X		
Taking photos on mobile phones cameras of children	X				X		
Taking photos on mobile phones cameras of inanimate objects		X			X		
Use of school email for personal use	X						
Use of personal email in school on school network	X				X		

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

- ❖ when communicating in a professional capacity, staff should ensure that the technologies they use are officially sanctioned by the school.
- ❖ any digital communication between staff and learners or parents/carers (e-mail, social media, learning platform, etc.) must be professional in tone and content.
- ❖ Personal e-mail addresses, text messaging or social media **must not** be used for these communications.
- ❖ staff should be expected to follow good practice when using personal social media regarding their own professional reputation and that of the school and its community
- ❖ users should immediately report to the Headteacher – in accordance with the school policy – the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- ❖ relevant policies (Code of Conduct and Online Safety within this policy) and permissions should be followed when posting information online e.g., school website and social media. Only school e-mail addresses should be used to identify members of staff and learners.

REPORTING AND RESPONDING

The school will take all reasonable precautions to ensure online safety for all school users but recognises that incidents may occur inside and outside of the school (with impact on the school) which will need intervention. The school will ensure:

- ❖ there are clear reporting routes which are understood and followed by all members of the school community which are consistent with the school safeguarding procedures, and with the whistleblowing, complaints and managing allegations policies. e.g. Report to DSL, Senior Leaders, Headteacher or Governor
- ❖ all members of the school community will be made aware of the need to report online safety issues/incidents
- ❖ reports will be dealt with as soon as is practically possible once they are received
- ❖ the Designated Safeguarding Lead/ Online Safety Lead and other responsible staff have appropriate skills and training to deal with online safety risks.
- ❖ if there is any suspicion that the incident involves any illegal activity or the potential for serious harm (see flowchart and user actions chart in the appendix), the incident must be escalated through the agreed school safeguarding procedures, this may include:
 - o Non-consensual images
 - o Self-generated images
 - o Terrorism/extremism
 - o Hate crime/ Abuse

- o Fraud and extortion
 - o Harassment/stalking
 - o Child Sexual Abuse Material (CSAM)
 - o Child Sexual Exploitation Grooming
 - o Extreme Pornography
 - o Sale of illegal materials/substances
 - o Cyber or hacking -offences under the Computer Misuse Act
 - o Copyright theft or piracy
- ❖ any concern about staff misuse will be reported to the Headteacher as per the Whistle blowing Policy, unless the concern involves the Headteacher, in which case the complaint is referred to the Chair of Governors and the local authority (LADO)
- ❖ for misuse of technology where there is no suspected illegal activity (either learners or adults), devices may be checked using the following procedures:
 - one or more senior members of staff should be involved in this process. This is vital to protect individuals if accusations are subsequently reported.
 - conduct the procedure using a designated device that will not be used by learners and, if necessary, can be taken off site by the police should the need arise (should illegal activity be subsequently suspected). Use the same device for the duration of the procedure.
 - ensure that the relevant staff have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
 - record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed, and attached to the form
 - once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
 - o internal response or discipline procedures
 - o involvement by local authority
 - o police involvement and/or action
- ❖ it is important that those reporting an online safety incident have confidence that the report will be treated seriously and dealt with effectively
- ❖ there are support strategies in place e.g., peer support for those reporting or affected by an online safety incident
- ❖ incidents should be logged on CPOMS/ Personnel file
- ❖ relevant staff are aware of external sources of support and guidance in dealing with online safety issues, e.g. local authority; police; CEOP.
- ❖ those involved in the incident will be provided with feedback about the outcome of the investigation and follow up actions (as relevant)

- ❖ learning from the incident (or pattern of incidents) will be provided (as relevant and anonymously) to:
 - the Safeguarding Team for consideration of updates to policies or education programmes and to review how effectively the report was dealt with
 - staff, through regular briefings
 - learners, through assemblies/lessons
 - parents/carers, through newsletters, school social media, website
 - governors, through regular safeguarding updates
 - local authority/external agencies, as relevant

The school will make the flowchart on the following page available to staff to support the decision-making process for dealing with online safety incidents.

Online Safety Incident Flowchart



SCHOOL ACTIONS

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with.

It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures as follows:

Responding to Learner Actions

Incidents	Refer to class teacher/tutor	Refer to Head of School/Senior leader/Online safety lead	Refer to Executive Headteacher	Refer to Police/Social Work	Refer to local authority technical support for advice/action	Inform parents/carers	Remove device/network/internet access rights	Issue a warning	Further sanction, in line with behaviour policy
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on User Actions on unsuitable/inappropriate activities).		X	X	X		X	X		X <i>If appropriate</i>
Attempting to access or accessing the school network, using another user's account (staff or learner) or allowing others to access school network by sharing username and passwords	X	X			X	X		X or	X
Corrupting or destroying the data of other users.	X	X			X	X			X
Sending an e-mail, text or message that is regarded as offensive, harassment or of a bullying nature		X				X	X		X
Unauthorised downloading or uploading of files or use of file sharing.		X			X	X	X		X <i>If appropriate</i>
Using proxy sites or other means to subvert the school's filtering system.		X	X		X	X	X		X <i>If appropriate</i>
Accidentally accessing offensive or pornographic material and failing to report the incident.	X	X			X	X		X	
Deliberately accessing or trying to access offensive or pornographic material.		X	X	X	X	X			X

Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act.		X	X		X	X		X	
Unauthorised use of digital devices (including taking images)	X	X				X		X	X
Unauthorised use of online services		X	X	X			X		
Actions which could bring the school into disrepute or breach the integrity or the ethos of the school.		X	X			X	X		X
Continued infringements of the above, following previous warnings or sanctions.			X		X	X	X		X

Responding to Staff actions

Incidents	Refer to Head of School	Refer to Executive Headteacher	Refer to local authority HR and or LADO	Refer to Police	Refer to LA / Technical Support Staff for action re filtering, etc.	Issue a 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	X
Deliberate actions to breach data protection or network security rules.		X	X		X		X	X
Deliberately accessing or trying to access offensive or pornographic material		X	X	X	X		X	X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		X	X	X	X		X	X
Using proxy sites or other means to subvert the school's filtering system.		X	X		X		X	X
Unauthorised downloading or uploading of files or file sharing	X		X		X	X		X
Breaching copyright or licensing regulations.	X	X	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 without permission	X		X		X	X		

Sending an e-mail, text or message that is regarded as offensive, harassment or of a bullying nature		x	x	x				x
Using personal e-mail/social networking/messaging to carry out digital communications with learners and parents/carers		x	x					x
Inappropriate personal use of the digital technologies e.g. social media / personal e-mail		x	x			x		
Careless use of personal data, e.g. displaying, holding or transferring data in an insecure manner	x		x		x	x		
Actions which could compromise the staff member's professional standing	x		x			x	x	x
Actions which could bring the school into disrepute or breach the integrity or the ethos of the school.		x	x			x	x	x
Failing to report incidents whether caused by deliberate or accidental actions	x		x			x		
Continued infringements of the above, following previous warnings or sanctions.		x	x			x	x	x

SOCIAL MEDIA

Expectations for teachers' professional conduct are set out in the DfE Teachers Standards but all adults working with children and young people must understand that the nature and responsibilities of their work place them in a position of trust and that their conduct should reflect this.

All schools and local authorities have a duty of care to provide a safe learning environment for learners and staff. Schools could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, bully online, discriminate on the grounds of sex, race, or disability or who defame a third party may render the school liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to learners through:

- ❖ ensuring that personal information is not published.
- ❖ education/training being provided including acceptable use, age restrictions, social media risks, digital and video images policy, checking of settings, data protection and reporting issues.
- ❖ clear reporting guidance, including responsibilities, procedures, and sanctions.
- ❖ risk assessment, including legal risk.
- ❖ guidance for learners, parents/carers

School staff should ensure that:

- ❖ No reference should be made in social media to learners, parents/carers or school staff.
- ❖ they do not engage in online discussion on personal matters relating to members of the school community.
- ❖ personal opinions should not be attributed to the school.
- ❖ security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.
- ❖ they act as positive role models in their use of social media

When official school social media accounts are established, there should be:

- ❖ a process for approval by senior leaders
- ❖ clear processes for the administration, moderation, and monitoring of these accounts – involving at least two members of staff
- ❖ a code of behaviour for users of the accounts
- ❖ systems for reporting and dealing with abuse and misuse
- ❖ understanding of how incidents may be dealt with under school disciplinary procedures.

PERSONAL USE

- ❖ personal communications are those made via personal social media accounts. In all cases, where a personal account is used which associates itself with, or impacts on, the school it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy
- ❖ personal communications which do not refer to or impact upon the school are outside the scope of this policy
- ❖ where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
- ❖ the school permits reasonable and appropriate access to personal social media sites during school hours e.g. break time and when children are off site.

MONITORING OF PUBLIC SOCIAL MEDIA

- ❖ As part of active social media engagement, the school may pro-actively monitor the Internet for public postings about the school.
- ❖ the school should effectively respond to social media comments made by others according to a defined policy or process.
- ❖ when parents/carers express concerns about the school on social media we will urge them to make direct contact with the school, in private, to resolve the matter. Where this cannot be resolved, parents/carers should be informed of the school complaints procedure.

DIGITAL AND VIDEO IMAGES

The development of digital imaging technologies has created significant benefits to learning, allowing staff and learners instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and learners need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for online bullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry 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 will inform and educate learners about the risks associated with the taking, use, sharing, publication and distribution of images.
- ❖ staff/volunteers must be aware of those learners whose images must not be taken/published. Those images should only be taken on school devices.

The personal devices of staff should not be used for such purposes

- ❖ in accordance with guidance from the Information Commissioner’s Office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone’s privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other learners in the digital/video images
- ❖ staff and volunteers are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, storage, distribution and publication of those images
- ❖ care should be taken when sharing digital/video images that learners are appropriately dressed
- ❖ learners must not take, use, share, publish or distribute images of others without their permission
- ❖ photographs published on the website, or elsewhere that include learners will be selected carefully and will comply with Online Safety Policy
- ❖ learners’ full names will not be used anywhere on a website or blog, particularly in association with photographs.
- ❖ written permission from parents or carers will be obtained before photographs of learners are taken for use in school or published on the school website/social media
- ❖ parents/carers will be informed of the purposes for the use of images, how they will be stored and for how long – in line with the school data protection policy
- ❖ images will be securely stored in line with the school retention policy

ONLINE PUBLISHING

The school communicates with parents/carers and the wider community and promotes the school through

- ❖ Public-facing website
- ❖ Social media – Instagram
- ❖ Online newsletters

The school website is managed/hosted by Juniper. The school ensures that online safety policy has been followed in the use of online publishing e.g., use of digital and video images, copyright, identification of young people, publication of school calendars and personal information – ensuring that there is least risk to members of the school community, through such publications.

Where learner work, images or videos are published, their identities are protected, and full names are not published.