Two Rivers Federation - ONLINE SAFETY POLICY

Scope of the Online Safety Policy

This Online Safety Policy outlines the commitment of Two Rivers Federation 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).

Two Rivers Federation 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.

Policy development, monitoring and review

This Online Safety Policy has been developed by the Computing lead in conjunction with Executive Head (DSL), Heads of School (Online Safety Leads) and Governing body.

Schedule for development, monitoring and review

This Online Safety Policy was approved by the *school governing body on:*	
The implementation of this Online Safety Policy will be monitored by:	Melanie Smallwood Karen Lintin Sarah Rushworth Liz Burnell
The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new technological developments, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	March 2027
Should serious online safety incidents take place, the following external persons/agencies should be informed:	LA safeguarding officer, police

Process for monitoring the impact of the Online Safety Policy

The school will monitor the impact of the policy using:

- *Cpoms logs of reported incidents*
- *Discussion with learners, staff, governing body, parents and carers*

Policy and leadership

Responsibilities

To ensure the online safeguarding of members of our school community it is important that all members of that community work together to develop safe and responsible online behaviours, learning from each other and from good practice elsewhere, reporting inappropriate online behaviours, concerns, and misuse as soon as these become apparent. While this will be a team effort, the following sections outline the online safety roles and responsibilities 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. A member of the governing body will take on the role of Safeguarding Governor. The role of the safeguarding Governor to include:

- regular meetings with the Designated Safeguarding Lead / Online Safety Lead
- regularly receiving (collated and anonymised) reports of online safety incidents
- checking that provision outlined in the Online Safety Policy (e.g. online safety education provision and staff training) is taking place as intended
- ensuring that the filtering and monitoring provision is reviewed and recorded, at least annually.
- reporting to relevant governors meeting.

Designated Safety Lead (DSL) / Executive Head

The day-to-day responsibility for online safety is held by the Designated Safeguarding Lead, as defined in Keeping Children Safe in Education.

The DSL / Executive Head will:

- hold the lead responsibility for online safety, within their safeguarding role.
- be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.
- ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role.
- will receive regular monitoring reports from the Online Safety Lead.
- meet regularly with the safeguarding governor to discuss current issues, review (anonymised) incidents including any filtering and monitoring incidents and ensuring that annual (at least) filtering and monitoring checks are carried out
- receive relevant and regularly updated training in online safety to enable them to understand the risks associated with online safety and be confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online
- ensure that the Online Safety Lead and other relevant staff carry out their responsibilities effectively and receive suitable training to enable them to carry out their roles and train other colleagues, as relevant.
- attend relevant governing body meetings
- report regularly to senior leadership team
- be responsible for receiving reports of online safety incidents and handling them and deciding whether to make a referral by liaising with relevant agencies, ensuring that all incidents are recorded.

- will work with the responsible Governor, IT service providers and computing subject leader in all aspects of filtering and monitoring.
- liaise with staff and IT providers on matters of safety and safeguarding and welfare (including online and digital safety)

Online Safety Leads / Heads of schools

The Online Safety Leads will:

- work closely on a day-to-day basis with the Designated Safeguarding Lead.
- be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.
- work with the responsible Governor, IT service providers and computing subject leader in all aspects of filtering and monitoring.
- receive reports of online safety issues, being aware of the potential for serious child protection concerns and ensure that these are logged to inform future online safety developments
- review and support the establishing of the school online safety policies
- promote an awareness of and commitment to online safety education / awareness raising across the school and beyond
- liaise with curriculum leaders to ensure that the online safety curriculum is planned, mapped, embedded and evaluated
- ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place and the need to immediately report those incidents
- provide (or identify sources of) training and advice for staff/governors/parents/carers/learners
- receive regularly updated training to allow them to understand how digital technologies are used and are developing (particularly by learners) with regard to the areas defined In Keeping Children Safe in Education:
    - content
    - contact
    - conduct
    - commerce

Curriculum Lead

Will work with the DSL/OSLs to:

- establish and review the school online safety policies
- to develop a planned and coordinated online safety education programme e.g. ProjectEVOLVE
  This will be provided through:
    - a discrete programme
    - PHSE and SRE programmes
    - A mapped cross-curricular programme
    - assemblies and pastoral programmes
    - through relevant national initiatives and opportunities e.g. Safer Internet Day
- monitor the use of technology in order that any misuse/attempted misuse can be reported to DSL or Online Safety Lead for investigation and action.

Senior Leaders

- will be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff
- work with the DSL, OSL, responsible Governor, IT service providers and computing subject leader in all aspects of filtering and monitoring.

Teaching and support staff

School staff are responsible for ensuring that:

- they have an awareness of current online safety matters/trends and of the current school Online Safety Policy and practices
- they understand that online safety is a core part of safeguarding
- they have read, understood, and marked as read the staff acceptable use agreement (AUA)
- they follow all relevant guidance and legislation including, for example, Keeping Children Safe in Education and UK GDPR regulations
- all digital communications with learners, parents and carers and others should be on a professional level and only carried out using official school systems
- they immediately report any suspected misuse or problem to the Executive Head (DSL), Heads of School (OSL) or computing subject leader for investigation/action, in line with the school safeguarding procedures
- online safety issues are embedded in all aspects of the curriculum and other activities
- learners understand and follow the Online Safety Policy and acceptable use agreements and are encouraged to adopt safe and responsible use both within and outside school
- they supervise and monitor the use of digital technologies, mobile devices, cameras, etc., in lessons and other school activities (where allowed) and implement current policies regarding these devices
- in lessons where internet use is pre-planned learners are 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 lessons take place using live-streaming or video conferencing, there is regard to national safeguarding guidance and local safeguarding policies
- there is a zero-tolerance approach to incidents of online-bullying, sexual harassment, discrimination, hatred etc
- they model safe, responsible, and professional online behaviours in their own use of technology, including out of school and in their use of social media.
- they adhere to the school's policies, regarding the use of devices, systems and passwords and have an understanding of basic cybersecurity
- they have a general understanding of how the learners in their care use digital technologies out of school, in order to be aware of online safety issues that may develop from the use of those technologies
- they are aware of the benefits and risks of the use of Artificial Intelligence (AI) services. Staff must ensure that guidelines/policies (pending) for AI use in school are adhered to – see 'the use of Artificial Intelligence (AI) systems in School' section in this policy

IT Provider

The IT Provider is responsible for ensuring that:

- they are aware of and follow the school Online Safety Policy to carry out their work effectively in line with school policy

- the school technical infrastructure is secure and is not open to misuse or malicious attack
- support the school to meet (as a minimum) the required online safety technical requirements as identified by the DfE Meeting Digital and Technology Standards in Schools & Colleges and guidance from local authority or other relevant body
- there is clear, safe, and managed control of user access to networks and devices
- they keep up to date with online safety technical information
- filtering and monitoring software/systems are implemented and regularly updated
- the filtering policy is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person

Learners

- are responsible for using the school digital technology systems in accordance with the learner acceptable use agreement and Online Safety Policy
- should understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- should know what to do if they or someone they know feels vulnerable when using online technology.
- should avoid plagiarism and uphold copyright regulations, taking care to protect the intellectual property of themselves and others and checking the accuracy of content
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school

Parents and carers

Parents and carers play a crucial role in ensuring that their children understand the need to use the online services and devices in an appropriate way.

The school will take every opportunity to help parents and carers understand these issues through:

- publishing the school Online Safety Policy and the learners' acceptable use agreement on the school website
- seeking their permissions concerning digital images, etc and their use of social media in relation to posts concerning the school
- parents/carers evenings, newsletters, website and information about national/local online safety campaigns and literature.

Professional Standards

There is an expectation that professional standards will be applied to online safety as in other aspects of school life.

Online Safety Policy

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
- is published on the school website

Acceptable use

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 / volunteer induction.
- Staff meetings.
- Communication with parents/carers.
- Built into education sessions.
- School website.

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, parents/carers (e-mail, social media, 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 a nominated person – 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 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.
- 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 the incident must be escalated through the agreed school safeguarding procedures
- any concern about staff misuse will be reported to the Executive Head, unless the concern involves the Executive Head, in which case the complaint is referred to the Chair of Governors and the local authority
- where there is no suspected illegal activity, 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 Cpoms (pupils) / Bromcom (staff)
    - 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
- 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 (pupils) / Bromcom (staff)
- relevant staff are aware of external sources of support and guidance in dealing with online safety issues, e.g. local authority; police; Reporting Harmful Content; CEOP.
- those involved in the incident will be provided with feedback about the outcome of the investigation and follow up actions
- learning from the incident (or pattern of incidents) will be provided to:
    - 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

A flowchart (see appendix 2) is available to staff to support the decision-making process for dealing with online safety incidents.

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; are to be logged and brought to the attention of the Executive Head, Head of School and Online Safety Lead.

The use of Artificial Intelligence (AI) systems in School

The federation acknowledges the potential benefits of the use of AI in an educational context - including enhancing learning and teaching, improving outcomes, improving administrative processes, reducing workload and preparing staff and learners for a future in which AI technology will be an integral part.

Currently the federation does not allow the use of AI tools to inform or improve teaching or administrative practices or procedures. Staff must adhere to this until an AI policy is in place (pending) and appropriate training and guidance has been provided.

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 e.g. SWGfL Project Evolve and regularly taught in a variety of contexts.

- lessons are matched to need; are age-related and build on prior learning
- lessons are context-relevant with agreed objectives. Learner need and progress are addressed through effective planning
- Digital competency is planned and effectively threaded through the appropriate digital pillars in other curriculum areas e.g. PHSE; SRE; Literacy etc
- it incorporates/makes use of relevant national initiatives and opportunities e.g. Safer Internet Day
- 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.
- learners 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 (including where the information is gained from Artificial Intelligence services)
- learners should be taught to respect copyright / intellectual property when using material accessed on the internet and particularly through the use of Artificial Intelligence services
- vulnerability is actively addressed as part of a personalised online safety curriculum e.g. for victims of abuse and SEND.
- learners should be helped to understand the need for the learner acceptable use agreement and encouraged to adopt safe and responsible use both within and outside school.
- staff should act as good role models in their use of digital technologies the internet and mobile devices
- in lessons where internet 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 internet searches
- where learners are allowed to freely search the internet, staff should be vigilant in supervising the learners and monitoring the content of the websites / tools the learners visit

Staff/volunteers

All staff will 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 and data protection training will be made available to all staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.
- the training will be an integral part of the school's annual safeguarding, data protection and cyber-security 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 will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations
- this Online Safety Policy and its updates will be presented to and discussed by staff in staff meetings
- the Designated Safeguarding Lead/Online Safety Lead/computing lead will provide advice / guidance / training to individuals as required.

Governors

Governors should take part in online safety training/awareness sessions,

This may be offered in several ways such as:

- attendance at training provided by the local authority or other relevant organisation
- participation in school training / information sessions for staff or parents
- Additional training will be made available to (at least) the Safeguarding Governor. This will include basic Cyber-security training, provided by DPO and 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 reviews.

Families

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

- Sharing useful information and links via newsletters.
- Reference to the relevant web sites/publications via the school web site.
- Parents/carers on-line safety training/sessions.
- High profile events/campaigns e.g. Safer Internet Day.
- Encouraging learners to pass on to parents the online safety messages they have learned in lessons

Technology

The school is 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. The school should ensure that all staff are made aware of policies and procedures in place on a regular basis and explain that everyone is responsible for online safety and data protection.

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
- the filtering and monitoring provision is reviewed (at least annually) by the Designated Safeguarding Lead, online safety and computing lead, 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 the Designated Safeguarding Lead, online safety and computing lead and a governor, in particular when a safeguarding risk is identified, there is a change in working practice or new technology is introduced

Filtering – statements to be reviewed with Itec

- the school manages access to content across its systems for all users and on all devices using the schools' internet provision. 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. These are acted upon in a timely manner, within clearly established procedures
- there is a clear process in place to deal with, and log, requests/approvals for filtering changes
- filtering logs are reviewed and the Designated Safeguarding Lead alerted to any breaches of the filtering policy, which are then acted upon
- there are regular checks of the effectiveness of the filtering systems. Checks are undertaken across a range of devices at least termly and the results recorded and analysed to inform and improve provision. The DSL and Governor are involved in the process and aware of the findings.
- devices that are provided by the school have school-based filtering applied.
- learners will use child friendly/age-appropriate search engines e.g. SWGfL Swiggle
- 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

Monitoring

The school follows the UK Safer Internet Centre Appropriate Monitoring guidance. The school has monitoring systems in place, agreed by senior leaders, to protect the school, systems and users:

- the school monitors 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 monitoring is in place.
- 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.
- guidelines and expectations for effective physical monitoring are regularly shared and discussed with all staff
- the monitoring provision is reviewed at least once every academic year and updated in response to changes in technology and patterns of online safety incidents and behaviours.

Technical Security

The school technical systems will be managed in ways that ensure that the school meets recommended standards in the DfE Technical Standards for Schools and Colleges (and others outlined in local authority policy and guidance):

- responsibility for technical security resides with SLT who may delegate activities to identified roles.
- 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. Users must immediately report any suspicion or evidence that there has been a breach of security
- password policy and procedures are implemented and are consistent with guidance from the National Cyber Security Centre
- all school networks, devices and system will be protected by secure passwords
- the administrator passwords for school systems are held securely
- there will be regular reviews and audits of the safety and security of school technical systems
- 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 up-to-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,
- computing lead / IT provider are 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
- use of school devices out of school and by family members is regulated by acceptable use statements that users consent to annually
- personal use of any device on the school network is regulated by acceptable use statements that users consent to annually
- staff members are not permitted to install software on a school-owned devices without the consent of the SLT/Computing lead/IT service provider
- removable media is not permitted unless approved by the SLT/Computing lead
- systems are in place to control and protect personal data and data is encrypted at rest and in transit
- guest users are provided with appropriate access to school systems based on an identified risk profile.
- dual-factor authentication is used for sensitive data or access outside of a trusted network
- systems are in place that prevent the unauthorised sharing of personal / sensitive data unless safely encrypted or otherwise secured
- staff must always recognise and safeguard sensitive data

Mobile technologies

The school acceptable use agreements for staff and learners outline the expectations around the use of mobile technologies.

The school allows:

	School devices	Personal devices

	School owned for individual use	School owned for multiple users	Authorised device	Student owned	Staff owned	Visitor owned
Allowed in school	**Yes**	**Yes**	**No**	No	Yes	Yes
Full network access	Yes	Yes	No	No	No	No
Internet only			No	No	Yes	Yes – guest wi-fi

School owned/provided devices:

- there is an asset log that clearly states whom a device has been allocated to
- any designated mobile-free zone is clearly signposted
- personal use (e.g. online banking, shopping, images etc.) is clearly defined and expectations are well-communicated
- the use of devices on trips/events away from school is clearly defined and expectation are well-communicated.
- liability for damage aligns with current school policy for the replacement of equipment.
- education is in place to support responsible use.

Personal devices:

- staff will not use personal mobile devices (including Smart watches) in school during teaching time or during any contact time with children or when there are children present
- devices must be in silent mode on the school site
- the use of personal mobile devices to photograph or video children is not permitted
- for school trips/events away from school, teachers will be permitted to use a personal mobile phone for emergencies. Teachers using their personal phone in an emergency will ensure that the number is hidden to avoid a parent/carer accessing a private phone number. A school device must still be used for any photographs or videos
- personal devices are brought into the school entirely at the risk of the owner and the decision to bring the device into the school lies with the user (and their parents/carers). The school accepts no responsibility or liability in respect of lost, stolen or damaged devices while at school or on activities organised or undertaken by the school
- where personal devices are used for school related work (e.g. checking school email, working on a device not owned by school) staff must ensure that GDPR policy and practice is adhered to
- there is clear advice and guidance at the point of entry for visitors to acknowledge school requirements

Social media (see social media and code of conduct policies)

Digital and video images

The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- the school may use live-streaming or video-conferencing services in line with national and local safeguarding guidance / policies.
- 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. Permission is not required for images taken solely for internal purposes
- 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
- learners' work can only be published with the permission of the learner and parents/carers

Online Publishing

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

- Public-facing website
- Social media
- Online newsletters

The school website is managed/hosted by eschools. 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.

Data Protection

Personal data will be recorded, processed, transferred, and made available according to the current data protection legislation.

The school:

- has a Data Protection Policy.
- implements the data protection principles and can demonstrate that it does so
- has paid the appropriate fee to the Information Commissioner's Office (ICO)
- has appointed an appropriate Data Protection Officer (DPO) who has effective understanding of data protection law and is free from any conflict of interest

For further information and guidance see GDPR policy and practice.

Cyber Security

**The school, with support from the DPO is currently reviewing the DfE Cyber security standards for schools and colleges and is working toward meeting these standards. There is a cyber security policy on draft form.*

- the school has reviewed the DfE Cyber security standards for schools and colleges and is working toward meeting these standards
- the school will conduct a cyber risk assessment annually and review each term
- the school, (*in partnership with their technology support partner),* has identified the most critical parts of the school's digital and technology services and sought assurance about their cyber security
- the school has an effective backup and restoration plan in place in the event of cyber attacks
- the school's governance and IT policies reflect the importance of good cyber security staff and Governors receive training on the common cyber security threats and incidents that schools experience the school's education programmes include cyber awareness for learners
- the school has a business continuity and incident management plan in place
- there are processes in place for the reporting of cyber incidents. All students and staff have a responsibility to report cyber risk or a potential incident or attack, understand how to do this feel safe and comfortable to do so.

To note:

The DfE Cyber security standards for schools and colleges explains:

The 'Cyber-security in schools: questions for governing bodies and Trustees' guidance produced by the National Cyber Security Centre (NCSC) aims to support governing bodies' and management committees' understanding of their education settings' cyber security risks. The guidance includes eight questions to facilitate the cyber security conversation between the governing body and school leaders, with the governing body taking the lead.

Acknowledgements:

SWGfL School Online Safety Policy Templates

Next review of On-line Safety policy March 2027