Two Rivers Federation

Online Safety Policy

This online safety policy has been developed in consultation with:

- Executive Head / Designated safeguard lead
- Heads of School
- Computing subject leader
- Online Safety Lead
- Governors

Scope of the Policy

This policy applies to all members of the school community (including staff, students/pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of school digital technology systems, both in and out of the school. It also applies to the use of personal digital technology on the school site.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of online-bullying or other online safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

The 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.

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.

Roles and Responsibilities

The following section outlines 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 has taken on the role of Safeguarding Governor The role of the Safeguard Governor will include:

- Regular meetings/feedback from the 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).
- Reporting to relevant Governors meeting.

Executive Head, Head of School and Senior Leaders –

- The Executive Head has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the Online Safety Lead and Computing subject leader and Head of School
- The Executive Head, Head of School and another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.
- The Executive Head is responsible for ensuring that the Online Safety Lead and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The Executive Head will 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.
- The Executive Head or Head of School will receive regular monitoring reports from the Online Safety Lead.

Online Safety Lead – Head of School in liaison with online safety co-ordinator

Updated guidance says:

- Takes day to day responsibility for online safety issues and with the computing subject leader has a role in establishing and reviewing the school online safety policies/documents.
- Ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- Promote an awareness of and commitment to online safety education / awareness raising across the school and beyond.
- Provide (or identify sources of) training and advice for staff/governors/parents/carers/learners.
- Receives reports of online safety incidents and creates a log of incidents to inform future online safety developments.
- Meets with Online Safety Governor to discuss current issues, review incident logs and filtering/change control logs.
- Reports any incidents to the Executive Head who will be responsible for the investigation, actioning and sanctioning of each incident.
- Liaise with technical staff, pastoral staff and support staff as required.

Computing Curriculum Lead

Curriculum Lead will work with the Online Safety Lead to develop a planned online safety education programme linked to the Education for a Connected World framework.

This will be provided through:

- A discrete programme linked to the 'Teach Computing' and Project EVOLVE units of work.
- PHSE.
- Assemblies.
- Through relevant national initiatives and opportunities e.g. Safer Internet Day.

Technical staff

The technical support provider (Itec) is responsible for ensuring:

- They are aware of and follow the school On-line Policy and 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.
- The school meets required online safety technical requirements as identified by the local authority or relevant body.
- There is a clear, safe and managed control of user access to networks and devices.

- They keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant.
- The use of technology is regularly and effectively monitored in order that any misuse/attempted misuse can be reported to the Executive Head / Head of school for investigation and action.
- That filtering and monitoring software/systems are implemented and regularly updated.

Teaching and Support Staff

Are responsible for ensuring that:

- They have an up to date awareness of online safety matters and of the current school online safety policy and practices.
- They have read, understood and signed the staff acceptable use policy/agreement.
- They report any suspected misuse or problem to the Executive Head, Head of School, Online Safety Lead, Computing subject leader for investigation/action/sanction.
- All digital communications with /pupils/parents/carers should be on a professional level and only carried out using official school systems.
- Online safety issues are embedded in all aspects of the curriculum and other activities.
- Pupils adhere to the Online Safety Policy and should be helped to understand the need for the pupil acceptable use agreement and encouraged to adopt safe and responsible use both within and outside school.
- Pupils have an understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- 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 with regard to these devices.
- In lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Have a zero tolerance approach to incidents of on-line 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.

Designated Safeguarding Lead

Should be trained in online safety issues and be aware of the potential for serious child protection/safeguarding issues to arise from:

- Sharing of personal data.
- Access to illegal/inappropriate materials.
- Inappropriate on-line contact with adults/strangers.
- Potential or actual incidents of grooming.
- Online-bullying.

Learners

- Are responsible for using the school digital technology systems in accordance with the pupil acceptable use policy and in-line with the 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 on-line technology.
- 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/carers

Parents/carers play a crucial role in ensuring that their children understand the need to use on-line services and devices in an appropriate way. The school will take every opportunity to help parents understand these issues through:

- Newsletters, school website and information about national/local online safety campaigns/literature.
- Publishing the school on-line policy and pupil acceptable use agreement on the school website.
- Seeking their permissions concerning digital images, cloud services etc.

Parents and carers will be encouraged to support the school in reinforcing the pupil acceptable use agreement and the on-line safety messages provided to leaners in school.

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.

The school has defined which on-line activities it regards as inappropriate in a school context and that users should not engage in these activities in or outside the school when using school equipment or systems. The school policy restricts usage as per the table of information in Appendix 2:1

Communication

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 school related **digital communication** between staff and pupils, parents/carers or others must be professional in tone and content. These communications may only take place on official school systems. Personal email addresses, text messaging or social media must not be used for these communications. Users should be aware that school email communications may be monitored.
- Video calls to communicate with pupils and/or parents/carers are permitted **during enforced periods of school closure**. For safeguarding purposes staff, pupils and parents/carers must follow the code of conduct and guidance as set out in acceptable use agreements – remote learning (see Appendix 1:1 and 1:2).
- Users must immediately report to the Executive Head or Head of school 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.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.
- 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.

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 or Head of school, 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
- 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.

- Incidents should be logged on cpoms (staff-safe)
- 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.
- Relevant staff are aware of external sources of support and guidance in dealing with online safety issues, e.g. local authority; police; Professionals Online Safety Helpline; Reporting Harmful Content; CEOP.
- Those involved in the incident will be provided with feedback about the outcome of the investigation and follow up actions (as relevant).

A flowchart (see appendix A9) is available to staff to support the decision-making process for dealing with online safety incidents.

Search, confiscation and file/data deletion

This refers only to the searching for and of electronic devices and the deletion of data/files on those devices.
The Executive Head has authorised the following members of staff to carry out searches for and of electronic devices and the deletion of data/files on those devices:
Heads of School
Learners: Pupils are not allowed to use mobile phones or other personal electronic devices during the school day.
Any devices brought into school by a child will be stored in the office until the end of the school day
If learners breach this rule:
Search for device – bags, coat pockets
Any electrical device will be confiscated and taken to the office.
Parents/carers will be informed that their child's device has been confiscated
Any confiscated device will be returned to the pupil or parent/carer at the end of day
School staff are reminded of the need to ensure the safe keeping of confiscated devices, to avoid the risk of compensation claims for damage/loss of such devices

School actions & sanctions

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 on Cpoms – and brought to the attention of the Executive Head, Head of School and Online Safety Lead.

Education and training

On-line Safety Education Program (currently being developed)

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 and regularly taught online safety curriculum for all year groups matched against a nationally agreed framework e.g. Education for a Connected World.
- 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
- Learner need and progress are addressed through effective planning and assessment
- Digital competency is planned and effectively threaded through other curriculum areas e.g. PHSE; SRE; Literacy etc
- It incorporates/makes use of relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week.
- The programme will be accessible to all learners.

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 training will be made available to 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 Schools' annual safeguarding and data protection training for all staff.
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school on-line 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 (or other nominated person) will receive regular updates through attendance at external training events (e.g. from SWGfL/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 in staff meetings/training sessions.
- The Online Safety Lead (or other nominated person) 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 a number of ways:

- 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 the Online safety Governor.

Parents/Carers

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

- Sharing on-line safety learning e.g. through class blogs.
- 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

The Wider Community

The school may provide opportunities for local community groups/members of the community to gain from the school's online safety knowledge and experience. This may be offered through the following:

- The school website will provide online safety information for parents and the wider community.
- Sharing their online safety expertise/good practice with other local schools.

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

- The school filtering policy statements are agreed by senior leaders and technical staff and are regularly reviewed and updated in response to changes in technology and patterns of online safety incidents/behaviour.
- The school manages access to content across its systems for all users, including access to on-line content and services. The filtering provided meets the standards defined in the UK Safer Internet Centre.
- Illegal content (e.g., child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC 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.
- There is a clear process in place to deal with requests for filtering changes.
- Learners will be encouraged to use child friendly/age-appropriate search engines e.g. SWGfL Swiggle.
- Filtering logs are regularly reviewed and alert the school to breaches of the filtering policy, which are then acted upon.

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.
- An appropriate monitoring strategy for all users has been agreed and users are aware that the network is monitored. There is a staff lead responsible for managing the monitoring strategy and processes.
- 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.
- Technical monitoring systems are up to date and managed and logs/alerts are regularly reviewed and acted upon.

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 strategy 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:

- All users have clearly defined access rights to school technical systems and devices.
- All users (at KS2 and above) will be provided with a username and password. Users are responsible for the security of their username and password. Users in KS1 will log-on with a class username and password.
- Users must immediately report any suspicion or evidence that there has been a breach of security
- All school networks and systems will be protected by secure passwords.
- There will be regular reviews of the safety and security of school technical systems.
- Servers, wireless systems and cabling must be securely located and physical access restricted.
- Appropriate security measures are in place through technical support services (Itec) 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 laptops are protected by up-to-date endpoint (anti-virus) software.
- Temporary access of 'guests', (e.g., trainee teachers, supply teachers, visitors) onto the school systems for work purposes will be granted with permission of the Executive Head.

- All staff will seek permission from the on-line safety or computing lead before installing software or programmes on school devices.
- All users must use encrypted memory sticks provided by the school on school devices.

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.
- The use of personal mobile devices to photograph or video children is not permitted.
- Devices must be in silent mode on the school site.
- Children are not permitted to use their own mobile devices or computing equipment in school. Any mobile device brought into school by a child will be stored in the office until the end of the school day. Smart watches must not be synced to phones during the school day.
- Volunteers, contractors, governors are not permitted to use personal mobile devices when on site during school hours. If this is required during school hours (e.g. for contractors to take photos of equipment or buildings), permission from the Executive Head or Head of school should be sought. Under no circumstances should they be used in the presence of children.
- Access to school systems using personal devices is not allowed or possible due to password protection unless permission has been granted by the Executive Head.
- 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.
- During periods of enforced school closure and remote learning staff are permitted to use their personal mobile phone or landline to contact parents/carers after permission has been sought from the Executive Head. Staff will ensure that the number is hidden to avoid a parent or student accessing a private phone number.
- Personal devices are brought into the school entirely at the risk of the owner and the decision to bring the device in to the school lies with the user (and their parents/carers) as does the liability for any loss or damage resulting from the use of the device in school.
- 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 (the school recommends insurance is purchased to cover that device whilst out of the home).
- 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.

Social media- protecting professional identity

See code of conduct

Monitoring of Public Social Media:

- As part of active social media engagement, it is considered good practice to 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.

Use of digital and video images

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Written permission from parents or carers will be obtained before digital/video images of pupils are published on the school website or local press.

- 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 pupils 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, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes.
- staff/volunteers must be aware of those learners whose images must not be taken/published.
- Care should be taken when taking digital/video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website, particularly in association with photographs.
- Pupil's work can only be published with the permission of the pupil and parents/carers.
- 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.
- The school may use live-streaming or video-conferencing services in line with national and local safeguarding guidance / policies.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the current data protection legislation.
The school must ensure that:

- It has a Data Protection Policy.
- It has paid the appropriate fee to the Information Commissioner's Office (ICO).
- It has appointed a Data Protection Officer (DPO).

For further information See **GDPR** policy and practice.

The online safety policy will be reviewed every 2 years, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be: March 2024

Acknowledgements:
SWGfL School Online Safety Policy Templates