360safe.org.uk
360safe@swgfl.org.uk

Online Safety Policy

Date	Reviewed by	Agreed by governors	Next due for review
September 2023	Helen Wallace	November 2023	October 2024
July 2025	South West Grid for Learning / HWallace	July 2025	July 2026

SWGFL-created

Statutory

1-year recommended review cycle

South West Grid for Learning Trust Ltd, Belvedere House, Woodwater Park, Pynes Hill, Exeter, EX2 5WS
Registered in England and Wales, Company Number 5589479. Charity Number 1120354. VAT Reg. Number 880 8618 88

Believe to achieve! "Roots will grow down into God's love and keep us strong." Eph 3:17

Values: Friendship, Respect, Trust, Courage, Perseverance, Compassion

Brinkworth Earl Danby's is committed to providing a secure, happy and stimulating learning environment in which EVERYONE is valued, spiritual growth is nurtured and potential maximised. We believe as a community that each child can reach their vocational potential. We believe each child is of unique worth made in the image of God. We believe in each child being the best that they can be and finding their place in the world. We believe in: a child's potential; being part of a community; being the best you can be.

In partnership with parents/carers, we aim to:

- create a happy, caring atmosphere in which each child feels secure and valued within an environment which is stimulating and attractive
- meet each child's needs physically, creatively, intellectually, emotionally and socially
- educate children about a diverse society and world in order to promote understanding and positive attitudes
- help the child acquire a set of moral and spiritual values that reflect our designation as a Church of England Voluntary Controlled Primary School
- inspire each child to be an enthusiastic learner and develop capabilities and attributes that 'build learning power'
- enable pupils to become confident and responsible citizens

Our ethos underpins our unique culture and behaviour in our Church of England School. Our children are at the centre of every decision made. We always ask 'of what benefit will this be to our children? Will this help support them to be the best they can be?' We go the extra mile. Whether it is staff, parents, children, governors or community members, we choose to make that extra effort for a better outcome for individuals and for our school community.

This policy is written with our vision, values, ethos and aims at its heart.

Policy Statement

The internet is an essential resource to support teaching and learning. The statutory curriculum requires pupils to learn how to locate, retrieve and exchange information using ICT. In delivering the curriculum, teachers need to plan to integrate the use of communications technology such as web-based resources and e-mail and mobile learning, such as phones. Computer skills are vital to access life-long learning and employment.

Young people have online access from many places - home, school, friends' homes, libraries and in some cases, mobile phones. Schools have a number of services to help ensure that curriculum use is safe and appropriate, however, access out of school does not usually have these services and has a range of risks associated with its use. Schools are ideally placed to help educate young people on online safety.

In line with school policies that protect pupils from other dangers, there is a requirement to provide pupils with as safe an online environment as possible and a need to teach them to be aware of, and respond responsibly to, the risks.

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

Brinkworth Earl Danby's CE Primary 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 takes place out of school.

Its aims are to protect learners from potential harm, both on and off-site and to demonstrate a commitment to appropriate use of digital technologies.

Roles and Responsibilities

The following sections outline the online safety roles and responsibilities of individuals and groups within the school.

Governors

The DfE guidance "Keeping Children Safe in Education" states:

"Governing bodies and proprietors should ensure there are appropriate policies and procedures in place in order for appropriate action to be taken in a timely manner to safeguard and promote children's welfare …. this includes … online safety"

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy e.g. by asking the questions posed in the UKCIS document "Online Safety in Schools and Colleges – questions from the Governing Body".

The Safeguarding-link Governor will carry out the following:

- regular meetings with the Designated Safeguarding Lead
- regularly receiving (collated and anonymised) reports of any online safety incidents
- Ensuring that the filtering and monitoring provision is reviewed and recorded, at least annually.
- reporting to relevant Governing Body Meetings
- Receiving (at least) basic cyber-security training

The governing body will also support the school in encouraging parents/carers and the wider community to become engaged in online safety activities.

Headteacher, Designated Safeguarding Lead and Deputies

- The headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community and fostering a culture of safeguarding, though the day-to-day responsibility for online safety is held by the Designated Safeguarding Lead, as defined in Keeping Children Safe in Education.
- The Headteacher, Designated Safeguarding Leads and Deputies 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 Headteacher, Designated Safeguarding Leads and Deputies 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 by assisting with termly filtering and monitoring checks.
- The headteacher/senior leaders will work with the Safeguarding-link Governor, DSL and deputies, Oakford (IT provider) in all aspects of filtering and monitoring.

Teaching and support staff

Curriculum Leads will work with the DSL to develop a planned and coordinated online safety education programme e.g. EVOLVE .

This will be provided through:

- assemblies and pastoral programmes
- through relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week.

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 signed the staff acceptable use agreement (AUA) included in this policy at Appendix 3
- they follow all relevant guidance and legislation including, for example, Keeping Children Safe in Education and UK GDPR regulations

- all digital communications with pupils, parents and carers and others should be on a professional level *and only carried out using official school systems and devices (where staff use AI, they should only use school-approved AI services for work purposes which have been evaluated to comply with organisational security and oversight requirements*
- they immediately report any suspected misuse or problem to the Designated Safeguarding Lead or deputies for investigation/action, in line with the school safeguarding procedures
- online safety issues are embedded in all aspects of the curriculum and other activities
- ensure pupils understand and follow the Online Safety Policy and acceptable use agreements, have a good 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 regarding these devices
- in lessons where internet use is pre-planned pupils 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 technical security policy, with regard to the use of devices, systems and passwords and have an understanding of basic cybersecurity
- they have a general understanding of how the pupils 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 in school, being transparent in how they use these services, prioritising human oversight. AI should assist, not replace, human decision-making. Staff must ensure that final judgments, particularly those affecting people, are made by humans, fact-checked and critically evaluated.

IT Provider

At Brinkworth Earl Danby's CE Primary School, our IT is managed by Oakford, it is the responsibility of the school to ensure that the provider carries out all the online safety measures that the school's obligations and responsibilities require. It is also important that the provider follows and implements school Online Safety Policy and procedures.

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
- there is 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 Headteacher / DSL or SBM for investigation and action
- the filtering policy is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person

Pupils

- are responsible for using the school digital technology systems in accordance with the learner acceptable use agreement included in this policy at Appendices 1 and 2 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 when using Artificial Intelligence (AI) services to protect the intellectual property of themselves and others and checking the accuracy of content accessed through AI services.
- 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

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

- publishing the school Online Safety Policy on the school website
- providing them with a copy of the pupils' acceptable use agreement
- publish information about appropriate use of social media relating to posts concerning the school.
- parents'/carers' evenings, newsletters, website, social media and information about national/local online safety campaigns and literature.

Community users

Community users who access school systems/website/learning platform as part of the wider school provision will have DBS clearance before being provided with access to school systems and Wi-Fi and will be expected to have appropriate regard for online safety.

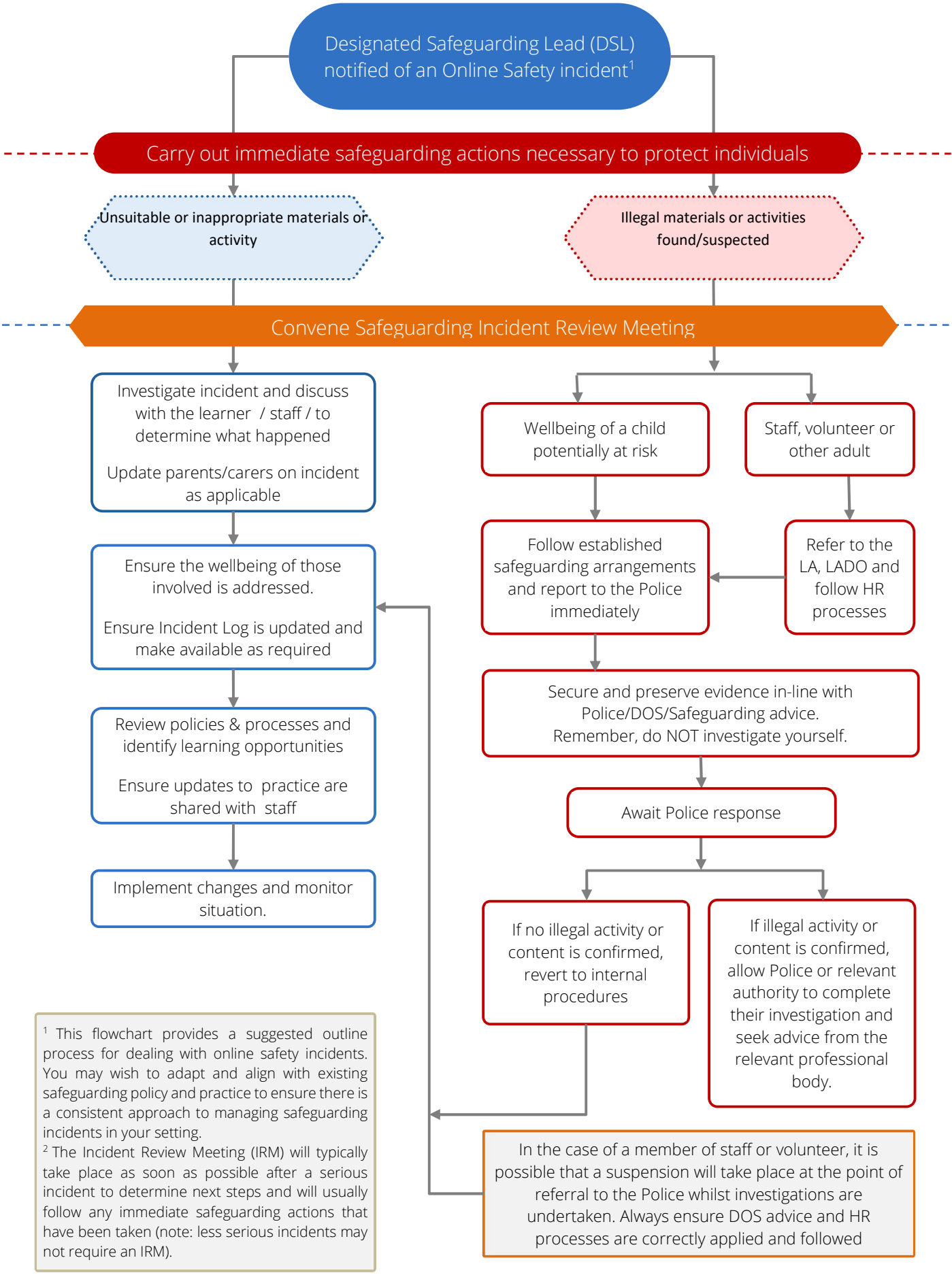
Reporting and responding

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:

- 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 and deputies and SBM 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:

  Non-consensual images
  Self-generated images
  Terrorism/extremism
  Hate crime/ Abuse
  Fraud and extortion
  Harassment/stalking
  Child Sexual Abuse Material (CSAM)
  Child Sexual Exploitation Grooming
  Extreme Pornography
  Sale of illegal materials/substances
  Cyber or hacking
  Copyright theft or piracy

- any concern about staff misuse will be reported to the Headteacher, unless the concern involves the Headteacher, in which case the complaint is referred to the Chair of Governors and the local authority / MATThe school will make the flowchart below available to staff to support the decision-making process for dealing with online safety incidents.



[1] This flowchart provides a suggested outline process for dealing with online safety incidents. You may wish to adapt and align with existing safeguarding policy and practice to ensure there is a consistent approach to managing safeguarding incidents in your setting.

[2] The Incident Review Meeting (IRM) will typically take place as soon as possible after a serious incident to determine next steps and will usually follow any immediate safeguarding actions that have been taken (note: less serious incidents may not require an IRM).

The use of Artificial Intelligence (AI) systems in School

As Generative Artificial Intelligence (gen AI) continues to advance and influence the world we live in , its role in education is also evolving. There are currently 3 key dimensions of AI use in schools: learner support, teacher support and school operations; ensuring all use is safe, ethical and responsible is essential.

We realise that there are risks involved in the use of Gen AI services, but that these can be mitigated through our existing policies and procedures, amending these as necessary to address the risks.

We will educate staff and pupils about safe and ethical use of AI, preparing them for a future in which these technologies are likely to play an increasing role.

The safeguarding of staff and pupils will, as always, be at the forefront of our policy and practice.

Filtering & Monitoring

The school filtering and monitoring provision is provided by Oakford who hold the technical responsibility, and is regularly reviewed (at least annually) and updated in response to changes in technology and patterns of online safety incidents/behaviours

The school currently have the Netsweeper filtering platform through Oakford Internet Services. A copy of the Netsweeper accreditation statement against the UKSIC guidelines (used within the DFE Filtering and Monitoring standards) can be found here.

https://d1xsi6mgo67kia.cloudfront.net/uploads/2016/09/Netsweeper-Appropriate-Filtering-Provider-Response-2023-Netsweeper-1.pdf

The Netsweeper platform technically can meet all requirements of the DFE standards. It's important to note that the school/Oakford should work together to ensure key points such as;

- Reporting has been configured to meet monitoring requirements outlined in the DFE's filtering and monitoring standards.
- Oakford, DSL, SLT and a responsible governor should meet once per year to review filtering and monitoring, including what is blocked/allowed and why on the system.
- The Netsweeper reports are checked termly and brief notes made on the Single Central Record (SCR) monitoring sheet.
- Random PC and Laptop history checks are also taken termly and noted on the SCR monitoring sheet.

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.

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.

Online Publishing

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

- Public-facing website
- Social media – own Facebook page
- Online newsletters

The school website is managed/hosted by Juniper Education. 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.

Cyber Security

The DfE Cyber security standards for schools and colleges explains:

"Cyber incidents and attacks have significant operational and financial impacts on schools and colleges. These incidents or attacks will often be an intentional and unauthorised attempt to access, change or damage data and digital technology. They could be made by a person, group, or organisation outside or inside the school or college and can lead to:

- safeguarding issues due to sensitive personal data being compromised
- impact on student outcomes
- a significant data breach
- significant and lasting disruption, including the risk of repeated future cyber incidents and attacks, including school or college closure
- financial loss
- reputational damage"

- 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
- the school, in partnership with Oakford, 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 and this is documented in the Business Continuity Plan
- 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 pupils
- 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.

Appendix A1 - Learner Acceptable Use Agreement – for KS2

I agree to use the school's digital systems safely and responsibly to protect me, other pupils and the school.

Keeping Safe Online

- The school will check how I use devices and the internet to keep everyone safe.
- I will keep my usernames and passwords private and tell a trusted adult if someone else knows them.
- I will be careful when talking to people online and will only talk to people I know and trust.
- I will not share personal information like my name, address, or photos without asking a trusted adult.
- I will only take or share images of myself, or others, when fully dressed.
- If I see or hear something online that worries or upsets me, I will tell a trusted adult straight away.
- I will only meet people I have spoken to online if a trusted adult is with me.

Using Computers and the Internet Sensibly

- I will only use devices, apps and sites that I am allowed to, and will check if I am unsure.
- I will always ask permission and check with a trusted adult before using someone else's work or pictures.

- I will make sure the information I find online is true by checking carefully.
- I will only use apps or tools, like AI, that my teacher has said are OK, and I will ask for help if I'm unsure.
- I will not copy or use music, videos, or games unless I have permission.
- I will tell a trusted adult about any damage to devices or if anything else goes wrong.
- I will check with trusted adults before clicking on any unexpected messages or links (even if these look as though they are from people that I already know).

Being Respectful and Responsible

- I will treat others kindly online, just as I do in real life.
- I will make good choices about what I share online to protect myself and others.
- I will spend a healthy amount of time using devices and make time for other activities too.
- I will always think about how my behaviour online could affect me, my friends, and my school.

What Happens If I Break These Rules

- If I don't follow these rules, my teacher may stop me from using computers or devices, speak to my parents, or take other actions to help me make better choices in the future.

By following these rules, I can enjoy using technology safely and responsibly.

I have read and understand the above and agree to follow these guidelines when:

- I use the school systems and devices (both in and out of school)
- I use my own devices in the school (when allowed) e.g. mobile phones, gaming devices USB devices, cameras etc.
- I am out of school and involved in any online behaviour that might affect the school or other members of the school.

Name of Learner: ..... Group/Class: .....

Signed: ..... Date: .....

A2 Learner Acceptable Use Agreement – for younger pupils (Early Years/KS1)

Our Technology Rules

I will follow these rules to use computers, tablets and the internet safely at school.

Staying Safe

- My teacher will watch what I do on computers, tablets and the internet to keep me safe.
- I will keep my passwords secret and tell my teacher if I need help.
- I understand that people online are not always who they say they are. I will only talk to people online if my teacher or a trusted adult says it's OK.
- I will not share my name, address, or pictures without asking my teacher or a trusted adult first.
- If I see something that makes me feel worried or upset, I will tell my teacher or a trusted adult straight away.
- I will only use apps, games or websites my teacher says are safe.

Using Technology Kindly

- I will be kind when using technology, just like I am in real life.
- I will take care of the computers and tablets I use.
- I will only look at things my teacher says are OK.

Making Good Choices

- I will ask my teacher before I use someone else's pictures or work.
- I will take breaks from screens and do other fun things too.
- I know that I can say no / please stop to anyone online who makes me feel sad, uncomfortable, embarrassed or upset.
- I will ask for help from a trusted adult if I am not sure what to do or if I think I may have done something wrong.

What Happens If I Forget the Rules

- If I forget the rules, my teacher will help me learn to make better choices next time.

These rules help us all stay safe and have fun using computers and tablets at school!

Signed (parent/carer): .....

A3Staff (and Volunteer/Other) Acceptable Use Agreement

The school will try to ensure that staff and volunteers will have good access to digital technology to enhance their work, to enhance learning opportunities and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school systems in a responsible way, to minimise the risk to the safety, privacy or security of the school community and its systems. I acknowledge the potential of digital technologies for enhancing learning and will endeavour to integrate them in a way that aligns with the school's policy, ethos and values.

For my professional and personal safety:

- I understand that the school monitors use of school technology
- I understand that the rules set out in this agreement also apply to use of these devices and technologies out of school, and to the transfer of personal / sensitive data (digital or paper based) out of the school
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password.
- I will store my passwords securely and in line with the school's relevant security policy.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the Headteacher / DSL or deputies.

I will be professional in my communications and actions when using digital technologies

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner. I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital/video images, and taking account of parental permissions. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the school website) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use social networking sites in the school in accordance with school policies.
- I will only communicate with pupils and parents/carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any online activity that may compromise my professional responsibilities.

The school has the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- I will abide by all relevant guidance and legislation (e.g., Keeping Children Safe in Education / UK GDPR)
- I will ensure that I am aware of cyber-security risks and that I will not respond to any communications that might put my / school data or systems at risk from attack
- When using AI systems in my professional role I will use these responsibly and:
  - will only use AI technologies approved by the school
  - will be aware of the risks of bias and discrimination, critically evaluating the outputs of AI systems for such risks
  - to protect personal and sensitive data, I will ensure that I have explicit authorisation when uploading sensitive school-related information into AI systems
  - will take care not to infringe copyright or intellectual property conventions – care will be taken to avoid intellectual property, including that of the pupils, being used to train generative AI models without appropriate consent.
  - ensure that documents, emails, presentations, and other outputs influenced by AI include clear labels or notes indicating AI assistance
  - critically evaluate AI-generated outputs to ensure that all AI-generated content is fact-checked and reviewed for accuracy before sharing or publishing
  - will use generative AI tools responsibly to create authentic and beneficial content, ensuring respect for individuals' identity and well-being
- When I use my personal mobile devices in school, I will follow the rules set out by the school, in the same way as if I was using school equipment. I will ensure that any such devices are protected by up to date anti-virus / anti-malware software and are free from viruses.
- I will exercise informed safe and secure practice when accessing links to content from outside of my organisation to reduce the risk of cyber security threats.
- I will ensure that my data is regularly backed up, in accordance with relevant school policies.
- I will not access illegal, inappropriate or harmful content on school systems.
- I will not bypass any filtering or security systems that are used to prevent access to such content.
- I will not install or attempt to install unauthorised programmes of any type on a school device , nor will I try to alter device settings, unless this is allowed in school policies
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the school Data Security Policy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based documents containing personal data must be held in lockable storage.
- I understand that the data protection policy requires that any staff or learner data to which I have access, will be kept private and confidential, except when it is deemed necessary that I

am required by law or by school policy to disclose such information to an appropriate authority.

- I will immediately report any damage or faults involving equipment or software, however this may have happened.

I understand that I am responsible for my actions in and out of the school:

- I understand that this acceptable use agreement applies to my use of digital technologies related to my professional responsibilities , within or outside of the school.
- I will ensure my use of technologies and platforms is in line with the school's agreed codes of conduct.
- I understand that if I fail to comply with this acceptable use agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and/or the Local Authority / Trust in the event of illegal activities, the involvement of the Police.

I have read and understand the above and agree to use the school digital technology systems (both in and out of the school) and my own devices (in the school and when carrying out communications related to the school) within these guidelines.

Staff/Volunteer/Other Name: .....

Signed: .....

Date: .....

The full Southwest Grid for Learning Online Safety Policy Guidance and templates is available to staff as a resource guide on the J: drive in Policies. This represents a summary of the items contained therein.

Copyright of the SWGfL School Online Safety Policy Templates is held by SWGfL. Schools and other educational institutions are permitted free use of the templates. Any person or organisation wishing to use the document for other purposes should seek consent from SWGfL and acknowledge its use.

Every reasonable effort has been made to ensure that the information included in this template is accurate, as at the date of publication in January 2025. However, SWGfL cannot guarantee its accuracy, nor can it accept liability in respect of the use of the material whether in whole or in part and whether modified or not. Suitable legal/professional advice should be sought if any difficulty arises in respect of any aspect of this new legislation or generally to do with school conduct or discipline.

© SWGfL 2025