SOLENT INFANT SCHOOL

Online Safety Policy

This 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 the school. It also applies to the use of personal digital technology on the school site (where allowed).

"We aim for all our children to develop a love of learning that will last them a lifetime, caring for and respecting the world around them, valuing differences and broadening moral values"

The Solent Schools, Vision, Values and Aims

Responsibility for policy review	Local Governing Body (LGB)
Date reviewed	10 December 2024
Review cycle	Annual. Next review: December 2025
Linked Policies	See Appendices, pages 32-57
Signature: *Chair of Governors*	**10 December 2024** *Date*

Contents

Online Safety Policy

Scope of the Online Safety Policy

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

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

Solent Infant 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.

Policy development, monitoring and review

This Online Safety Policy has been developed by the Digital Strategy Leads made up of:
- Executive Headteacher
- Designated safeguarding lead (DSL)
- Online Safety Lead (OSL)
- Network Manager
- Governor Lead for Digital Strategy
- Computing Leads
- Parents and carers

Consultation with the whole school community has taken place through a range of formal and informal communication.

Schedule for development, monitoring and review

This Online Safety Policy was approved by the school governing body on:	10 December 2024
The implementation of this Online Safety Policy will be monitored by:	• Designated Safeguarding Lead • Executive Headteacher • Network Manager • Governor Lead for Digital Strategy
Monitoring will take place at regular intervals:	• Termly Digital Strategy Meetings (at least) • Full review annually • Behaviour & Safety Governing Body Meetings termly
The governing body will receive a report on the implementation of the Online Safety Policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals:	• Termly Headteacher's Report to Governors and Trustees

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:	09.12.2025
Should serious online safety incidents take place, the following external persons/agencies should be informed:	• Darren Failes - Trust Operations Manager • Sara Spivey – De Curci Trust CEO • PCC Multi Agency Safeguarding Team • Police

Process for monitoring the impact of the Online Safety Policy

The school will monitor the impact of the policy using:

- Logs of reported incidents.
- Filtering and monitoring logs.
- Internal monitoring data for network activity.
- Surveys/questionnaires of:
  - learners
  - parents and carers
  - volunteers
  - Staff

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.

Executive Headteacher and senior leaders

- The Executive 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 Executive Headteacher and (at least) 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 [1]
- The Executive Headteacher/senior leaders are responsible for ensuring that the Designated Safeguarding Lead / Online Safety Lead, Network Manager, 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.
- The Executive Headteacher/senior leaders 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 Headteacher/senior leaders will receive regular monitoring reports from the Designated Safeguarding Lead / Online Safety Lead.
- The Executive Headteacher/senior leaders will work with the responsible Governor, the Designated Safeguarding Lead (DSL), and the Network Manager in all aspects of filtering and monitoring.

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"

"Governing bodies and proprietors should ensure an appropriate senior member of staff, from the school or college leadership team, is appointed to the role of designated safeguarding lead. The designated safeguarding lead should take lead responsibility for safeguarding and child protection (including online safety and understanding the filtering and monitoring systems and processes in place)"

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".

This review will be carried out by the Behaviour and Safety Committee, whose members will receive regular information about online safety incidents and monitoring reports. A member of the governing body will take on the role of Online Safety 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)

---

[1] See flow chart on dealing with online safety incidents in 'Responding to incidents of misuse' and relevant local authority/MAT/ HR/other relevant body disciplinary procedures.

- ensuring that the filtering and monitoring provision is reviewed and recorded, at least annually - the review will be conducted by members of the SLT, the DSL, and the Network Manager and involve the responsible governor – in line with the [DfE Filtering and Monitoring Standards](#)
- reporting to relevant governing body meetings
- receiving (at least) basic cyber-security training to enable the governors to check that the school meets the [DfE Cyber-Security Standards](#)
- membership of the school Online Safety Group (Community Focus Group)

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

Designated Safety Lead (DSL)

Keeping Children Safe in Education states that:

> *"The designated safeguarding lead should take lead responsibility for safeguarding and child protection (including online safety and understanding the filtering and monitoring systems and processes in place). This should be explicit in the role holder's job description."*

> They (the DSL) *"are able to understand the unique 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 at school or college"*

> They (the DSL) *"can recognise the additional risks that children with special educational needs and disabilities (SEND) face online, for example, from bullying, grooming and radicalisation and are confident they have the capability to support children with SEND to stay safe online"*

The DSL (who is also the OSL) will:
- Hold the lead responsibility for online safety, within their safeguarding role.
- 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.
- Meet regularly with the online safety governor to discuss current issues, review (anonymised) incidents and filtering and monitoring logs and ensuring that annual (at least) filtering and monitoring checks are carried out.
- Attend relevant governing body meetings/groups.
- Report regularly to Executive Headteacher/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.
- Liaise with staff and Network Manager on matters of safety and safeguarding and welfare (including online and digital safety)

In their role as OSL:

- Lead the Online Safety Group
- 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.
- Have a leading role in establishing and reviewing the school online safety policies/documents.
- 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.
- Liaise with (school/local authority/MAT/external provider) technical staff, pastoral staff and support staff (as relevant).
- Receive regularly updated training to allow them to understand how digital technologies are used and are developing (particularly by learners) regarding the areas defined In Keeping Children Safe in Education:
  - content
  - contact
  - conduct
  - commerce

Curriculum Leads

Curriculum Leads will work with the DSL/OSL to develop a planned and coordinated online safety education programme.

This will be provided through:

- A discrete programme.
- PHSE and SRE programmes.
- A mapped cross-curricular programme.
- Assemblies and pastoral programmes.
- Themed weeks and days (both national and school led) e.g. Safer Internet Day and Anti-bullying week.

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 signed the DCT staff acceptable use agreement (AUA)
- They immediately report any suspected misuse or problem to the Designated Safeguarding Lead for investigation/action, in line with the school safeguarding procedures.
- All digital communications with learners and parents/carers are on a professional level and only carried out using official school systems such as Arbor, Tapestry or Microsoft Teams.
- Online safety issues are embedded in all aspects of the curriculum and other activities.
- Ensure learners 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 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 videoconferencing, 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.

Network Manager (Solent IT Service Provider)

The DfE Filtering and Monitoring Standards says:

"Senior leaders should work closely with governors or proprietors, the designated safeguarding lead (DSL) and IT service providers in all aspects of filtering and monitoring. Your IT service provider may be a staff technician or an external service provider."

"Day to day management of filtering and monitoring systems requires the specialist knowledge of both safeguarding and IT staff to be effective. The DSL should work closely together with IT service providers to meet the needs of your setting. You may need to ask filtering or monitoring providers for system specific training and support."

"The IT service provider should have technical responsibility for:
- *maintaining filtering and monitoring systems*
- *providing filtering and monitoring reports*
- *completing actions following concerns or checks to systems"*

"The IT service provider should work with the senior leadership team and DSL to:

- *procure systems*
- *identify risk*
- *carry out reviews*
- *carry out checks"*

The Network Manager is responsible for ensuring that:

- They are aware of and follow the school Online Safety Policy and Technical Security 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
- The school meets (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 / MAT 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 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 Designated Safeguarding Lead / Online Safety Lead (shared role at Solent) 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.
- Monitoring systems are implemented and regularly updated as agreed in school policies.

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 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 on the school website
- Providing them with a copy of the learners' acceptable use agreement.

- Publish information about appropriate use of social media relating to posts concerning the school.
- Seeking their permissions concerning digital images, cloud services etc.
- Parents'/carers' evenings, newsletters, website, social media and information about national/local online safety campaigns and literature.

Parents and carers will be encouraged to support the school in:
- Reinforcing the online safety messages provided to learners in school.
- The safe and responsible use of their children's personal devices in the school (where this is allowed).
- Consider appropriate use of social media (including WhatsApp groups) concerning the school.

Community users

Community users who access school systems/website/learning platform as part of the wider school provision will be expected to sign a community user AUA before being provided with access to school systems.

Online Safety Group (part of the wider safeguarding group)

The Online Safety Group at Solent is contained within the safeguarding group and provides a consultative group that has wide representation from the school community, with responsibility for issues regarding online safety and monitoring the Online Safety Policy including the impact of initiatives.

The Online Safety Group has the following members:
- Designated Safeguarding Lead / Online Safety Lead.
- Senior leaders.
- Online Safety Digital Lead governor.
- Network Manager.
- Representative parents/carers (where appropriate)

Members of the Online Safety Group will assist the DSL/OSL with:
- The production/review/monitoring of the school Online Safety Policy/documents.
- The production/review/monitoring of the school filtering policy and requests for filtering changes.
- Mapping and reviewing the online safety education provision – ensuring relevance, breadth and progression and coverage.
- Reviewing network/filtering/monitoring/incident logs, where possible.
- Encouraging the contribution of learners to staff awareness, emerging trends and the school online safety provision.
- Consulting stakeholders – including staff/parents/carers - about the online safety provision.
- Monitoring improvement actions identified through use of the 360-degree safe self-review tool.

Online Safety Policy

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

"Online safety and the school or college's approach to it should be reflected in the child protection policy"

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 such as whole staff updates, shared networks, and iAMCompliant.
- is published on the school website.

Acceptable use

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

Acceptable use agreements

An Acceptable Use Agreement is a document that outlines a school's expectations on the responsible use of technology by its users. The staff acceptable use agreement (AUA) is read and signed by staff as part of their conditions of employment during the induction process. The Online Safety Policy and acceptable use agreements define acceptable use at the school. The acceptable use agreements will be communicated/re-enforced through:

- staff induction and handbook
- digital signage
- posters/notices around where technology is used
- communication with parents/carers
- built into education sessions
- school website
- peer support.

The following table outlines what is considered acceptable at Solent Infant School:

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

Consideration has been given for the following activities when undertaken for non-educational purposes:	Staff and other adults				Learners			
	Not allowed	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission/awareness
Online gaming								
Online shopping/commerce								
File sharing								
Social media								
Messaging/chat								
Entertainment streaming e.g. Netflix, Disney+								With staff permission
Use of video broadcasting, e.g. YouTube, Twitch, TikTok								With staff permission
Mobile phones may be brought to school								Upper key stage 2 – switched off and in class locker
Use of mobile phones for learning at school								
Use of mobile phones in social time at school								
Taking photos on mobile phones/cameras								
Use of other personal devices, e.g. tablets, gaming devices								
Use of personal e-mail in school, or on school network/wi-fi								
Use of school e-mail for personal e-mails								

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

- When communicating in a professional capacity, staff should ensure that the technologies they use are officially sanctioned by the school.
- Any digital communication between staff and learners or parents/carers (e-mail, social media, learning platform, etc.) must be professional in tone and content. Personal e-mail addresses, text messaging or social media must not be used for these communications.
- Staff should be expected to follow good practice when using personal social media regarding their own professional reputation and that of the school and its community.
- Users should immediately report to 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.
- 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 via Safeguard My School

- reports will be dealt with as soon as is practically possible once they are received

- the Designated Safeguarding Lead / Online Safety Lead and other responsible staff have appropriate skills and training to deal with online safety risks.

- if there is any suspicion that the incident involves any illegal activity or the potential for serious harm (see flowchart and user actions chart in the appendix), the incident must be escalated through the agreed school safeguarding procedures, this may include
  o Non-consensual images
  o Self-generated images
  o Terrorism/extremism
  o Hate crime/ Abuse
  o Fraud and extortion
  o Harassment/stalking
  o Child Sexual Abuse Material (CSAM)
  o Child Sexual Exploitation Grooming
  o Extreme Pornography
  o Sale of illegal materials/substances
  o Cyber or hacking
  o Copyright theft or piracy

- any concern about staff misuse will be reported to the Executive Headteacher, unless the concern involves the Executive Headteacher, in which case the complaint is referred to the Chair of Governors and the De Curci Trust CEO

- 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 the form
- once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
  - internal response or discipline procedures
  - involvement by the De Curci Trust
  - police involvement and/or action
- it is important that those reporting an online safety incident have confidence that the report will be treated seriously and dealt with effectively
- there are support strategies in place e.g., peer support for those reporting or affected by an online safety incident
- incidents should be logged on Safeguard My School
- 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.
- learning from the incident (or pattern of incidents) will be provided (as relevant and anonymously) to:
  - the Online Safety Group for consideration of updates to policies or education programmes and to review how effectively the report was dealt with
  - staff, through regular briefings
  - learners, through assemblies/lessons
  - parents/carers, through newsletters, school social media, website
  - governors, through regular safeguarding updates
  - external agencies such as Portsmouth Multi Agency Safeguarding Hub (as relevant)

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

Online Safety Incident Flowchart

Unsuitable materials or activity

Report to the Designated Safeguarding Lead (DSL) who also has responsibility for Online Safety

If staff/volunteer or learner; review the incident and decide upon the appropriate course of action.

Debrief on online safety incident.

Record details in incident log

Review polices and share experiences and practice as required.

Keep incident log up to date and make available to the De Curci Trust, Governing Body etc. as required.

Implement changes.

Monitor situation.

The DSL is responsible for wellbeing and as such should be informed of anything that places a child at risk, BUT safeguarding procedures must be followed.

Illegal materials or activities found or suspected.

Initial review/Professional strategy meeting with Designated Safeguarding Lead (DSL) & Senior team

Report to Police and report under local safeguarding arrangements.
DO NOT DELAY, if you have any concerns, report them immediately.

Secure and preserve evidence.
Remember do not investigate yourself. Do not ask leading questions'.

Await Police response.

If no illegal activity or material is confirmed, then revert to internal procedures.

If illegal activity or materials are confirmed, allow Police or relevant authority to complete their investigation and seek advice from the relevant professional body.

In the case of a member of staff or volunteer, it is likely that a suspension will take place at the point of referral to police, whilst police and internal procedures are being undertaken.

School actions

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures as follows:

Responding to Learner Actions *(identified lead is first point of contact & may then escalate further following investigation)*

Incidents	Refer to class teacher/tutor	Refer to Head of School (In role as DSL & OSL)	Refer to Executive Headteacher	Refer to Police/Social Work	Refer to the De Curci Trust IT Operations Manager	Inform parents/carers	Remove device/network/internet access rights	Issue a warning	Further sanction, in line with behaviour policy
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on User Actions on unsuitable/inappropriate activities		X	X	X	X	X	X		X
Attempting to access or accessing the school network, using another user's account (staff or learner) or allowing others to access school network by sharing username and passwords		X			X	X			X
Corrupting or destroying the data of other users.			X		X	X		X	X
Sending an e-mail, text or message that is regarded as offensive, harassment or of a bullying nature		X				X		X	X
Unauthorised downloading or uploading of files or use of file sharing.		X				X			X
Using proxy sites or other means to subvert the school's filtering system		X	X		X	X	X		X
Accidentally accessing offensive or pornographic material and failing to report the incident		X			X	X			X
Deliberately accessing or trying to access offensive or pornographic material.		X	X	X	X	X	X		X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act.			X		X	X			X
Unauthorised use of digital devices (including taking images)		X				X			X
Unauthorised use of online services		X				X			X
Actions which could bring the school into disrepute or breach the integrity or the ethos of the school.			X			X			X
Continued infringements of the above, following previous warnings or sanctions			X		X	X			X

Responding to Staff Actions *(nominated staff lead is initial staff contact and may choose to escalate further)*

Incidents	Refer to manager	Refer to Executive Headteacher and DSL (Head of School)	Refer to De Curci Trust IT Operations Manager	Refer to Local Authority Designated Officer (LADO) and/or police	Refer to Network Manager for action re filtering, etc	Issue a warning (if first offence and as a minimum)	Immediate suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities)		X		X				X
Deliberate actions to breach data protection or network security rules.		X	X	X				X
Deliberately accessing or trying to access offensive or pornographic material		X	X	X				X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software			X			X		
Using proxy sites or other means to subvert the school's filtering system.		X	X	X				X
Unauthorised downloading or uploading of files or file sharing			X		X	X		
Breaching copyright or licensing regulations.					X	X		
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account.		X			X	X		
Sending an e-mail, text or message that is regarded as offensive, harassment or of a bullying nature		X				X		
Using personal e-mail/social networking/messaging to carry out digital communications with learners and parents/carers		X	X	X				X
Inappropriate personal use of the digital technologies e.g. social media / personal e-mail		X	X			X		
Careless use of personal data, e.g. displaying, holding or transferring data in an insecure manner		X			X	X		
Actions which could compromise the staff member's professional standing		X				X		
Actions which could bring the school into disrepute or breach the integrity or the ethos of the school.		X						X
Failing to report incidents whether caused by deliberate or accidental actions		X	X					X
Continued infringements of the above, following previous warnings or sanctions		X	X	X				X

Online Safety Education Programme

While regulation and technical solutions are particularly important, their use must be balanced by educating learners to take a responsible approach. The education of learners in online safety is therefore an essential part of the school's online safety provision. Learners need the help and support of the school to recognise and avoid online safety risks and develop their resilience.

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. Education for a Connected Work Framework by UKCIS/DCMS and the 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 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 the appropriate digital pillars in other curriculum areas e.g. PHSE; SRE; Literacy etc.

- It incorporates and makes use of relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week

- The programme will be accessible to learners at different ages and abilities such as those with additional learning needs or those with English as an additional language.

- Vulnerability is actively addressed as part of a personalised online safety curriculum e.g., for victims of abuse and SEND.

- Acceptable use is reinforced across the curriculum, with opportunities to discuss how to act within moral and legal boundaries online, with reference to the Computer Misuse Act 1990.

- 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 the young people visit.

- It is accepted that from time to time, for good educational reasons, students may need to research topics, (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff should be able to request the temporary removal of those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

- The online safety education programme should be relevant and up to date to ensure the quality of learning and outcomes.

Contribution of Learners

The school acknowledges, learns from, and uses the skills and knowledge of learners in the use of digital technologies. We recognise the potential for this to shape the online safety strategy for the school community and how this contributes positively to the personal development of young people. Their contribution is recognised through:

- mechanisms to canvass learner feedback and opinion.

- appointment of digital leaders/teach peace/ play pal pupils /peer mentors

- the Online Safety Group has learner representation through pupil/school council meetings and discussions

- learners contribute to the online safety education programme e.g. peer education, digital leaders

- contributing to online safety events with the wider school community e.g. parents' evenings, family learning programmes etc.

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 and data protection training for all staff

- all new staff will receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and acceptable use agreements. It includes explicit reference to classroom management, professional conduct, online reputation and the need to model positive online behaviours.

- the Online Safety Lead and Designated Safeguarding Lead (or other nominated person) will receive regular updates through attendance at external training events, (e.g. UKSIC / SWGfL / MAT / LA / other relevant organisations) and by reviewing guidance documents released by relevant organisations

- this Online Safety Policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days

- the Designated Safeguarding Lead/Online Safety Lead will provide advice/guidance/training to individuals as required.

Governors

Governors should take part in online safety training/awareness sessions, with particular importance for those who are members of any sub-committee/group involved in technology / online safety / health and safety / safeguarding. This may be offered in several ways such as:

- attendance at training provided by the local authority/MAT or other relevant organisation
- participation in school training / information sessions for staff or parents

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

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

Families

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

- regular communication, awareness-raising and engagement on online safety issues, curriculum activities and reporting routes
- regular opportunities for engagement with parents/carers on online safety issues through awareness workshops / parent/carer evenings etc
- the learners – who are encouraged to pass on to parents the online safety messages they have learned in lessons and by learners leading sessions at parent/carer evenings
- letters, newsletters, website, Teams / Tapestry
- high profile events / campaigns e.g. Safer Internet Day
- reference to the relevant web sites/publications

Adults and Agencies

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

- online safety messages targeted towards families and relatives.
- providing online safety information via their website and social media for the wider community
- supporting community groups, e.g. early years settings, childminders, youth/sports/voluntary groups to enhance their online safety provision

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, Trust IT Operations Manager and the IT Network Manager and is regularly reviewed (at least annually) and updated in response to changes in technology and patterns of online safety incidents/behaviours

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

The filtering and monitoring provision is reviewed at least annually by senior leaders, the Designated Safeguarding Lead and a governor with the involvement of the IT Network Manager.

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

Filtering

- the school manages access to content across its systems for all users and on all devices using the school's 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
- there is a clear process in place to deal with, and log, requests/approvals for filtering changes (see Appendix for more details).
- filtering logs are regularly reviewed and alert the Designated Safeguarding Lead to breaches of the filtering policy, which are then acted upon.
- access to content through non-browser services (e.g. apps and other mobile technologies) is managed in ways that are consistent with school policy and practice.

If necessary, the school will seek advice from, and report issues to, the SWGfL Report Harmful Content site.

Monitoring

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

- the school monitors all network use across all its devices and services
- monitoring reports are urgently picked up, acted on and outcomes are recorded by the Designated Safeguarding Lead, all users are aware that the network (and devices) are monitored
- there are effective protocols in place to report abuse/misuse. There is a clear process for prioritising response to alerts that require rapid safeguarding intervention
- management of serious safeguarding alerts is consistent with safeguarding policy and practice.

The school follows the UK Safer Internet Centre Appropriate Monitoring guidance and protects users and school systems using the appropriate blend of strategies informed by the school's risk assessment. These may include:

- physical monitoring (adult supervision in the classroom)
- internet use is logged, regularly monitored and reviewed
- filtering logs are regularly analysed, and breaches are reported to senior leaders
- pro-active alerts inform the school of breaches to the filtering policy, allowing effective intervention
- where possible, school technical staff regularly monitor and record the activity of users on the school technical systems
- use of a third-party assisted monitoring service to review monitoring logs and report issues to school monitoring lead(s)

Technical Security

The school technical systems will be managed in ways that ensure that the school meets recommended technical requirements. Please refer to The De Curci Trust IT Operations Handbook for further information.

Mobile technologies

The school/trust acceptable use agreements for staff/volunteers, learners, parents, and carers 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 device²	Student owned	Staff owned	Visitor owned
Allowed in school	Yes	Yes	Yes	No*	Yes	Yes
Full network access	Yes	Yes	Yes	No	Yes	No
Internet only				No	Yes	Yes
No network access				No		

∗ *Solent Junior School Year 5 and 6 pupils are allowed to bring mobile phones into school if they are turned off and stored in a locked (school managed) space whilst on site.*

School owned/provided devices:

- all school devices are managed though the use of Mobile Device Management software
- there is an asset log that clearly states whom a device has been allocated to. There is clear guidance on where, when and how use is allowed
- 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.

Personal devices:

- there is a clear policy covering the use of personal mobile devices on school premises for all users
- where personal devices are brought to school, but their use is not permitted, appropriate, safe and secure storage will be made available
- use of personal devices for school business is defined in the acceptable use policy
- the expectations for taking/storing/using images/video aligns with the school's acceptable use policy and use of images/video policy. The non-consensual taking/using of images of others is not permitted
- liability for loss/damage or malfunction of personal devices is clearly defined
- there is clear advice and guidance at the point of entry for visitors to acknowledge school requirements
- education about the safe and responsible use of mobile devices is included in the school online safety education programmes as appropriate

Please refer to The De Curci Trust Staff Acceptable Use Policy for further details.

---

2 Authorised device – purchased by the learner/family through a school-organised scheme. This device may be given full access to the network as if it were owned by the school.

Social media

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

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

School staff should ensure that:

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

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

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

Personal use

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

Monitoring of public social media

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

School use of social media for professional purposes will be checked regularly by a senior leader and the Online Safety Lead to ensure compliance with the social media, data protection, communications, digital image and video policies. In the event of any social media issues that the school is unable to resolve support may be sought from the Professionals Online Safety Helpline.

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 in not covered by the Data Protection Act), unless explicitly asked not to at the event. 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 school social media, particularly in association with photographs

- written permission from parents or carers will be obtained upon starting Solent Infant School, 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

Online Publishing

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

- Public-facing website
- Social media
- Online newsletters
- Tapestry in EYFS
- Email and Messaging Systems (MIS)

The school website is managed by the school Network Manager and hosted by EUK Host. 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 learners' 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 (De Curci Trust 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 – Trust based) who has effective understanding of data protection law and is free from any conflict of interest.
- has a 'Record of Processing Activities' in place and knows exactly what personal data is held, where, why and which member of staff has responsibility for managing it
- the Record of Processing Activities lists the lawful basis for processing personal data (including, where relevant, consent). Where special category data is processed, an additional lawful basis is listed

- has an 'information asset register' in place and knows exactly what personal data is held, where, why and which member of staff has responsibility for managing it
- information asset register lists the lawful basis for processing personal data (including, where relevant, consent). Where special category data is processed, an additional lawful basis will have also been listed
- will hold the minimum personal data necessary to enable it to perform its function and will not hold it for longer than necessary for the purposes it was collected for. The school 'retention schedule' supports this
- data held is accurate and up to date and is held only for the purpose it was held for. Systems are in place to identify inaccuracies, such as asking parents to check emergency contact details at suitable intervals
- provides staff, parents, volunteers, with information about how the school looks after their data and what their rights are in a clear Privacy Notice
- has procedures in place to deal with the individual rights of the data subject, e.g. one of the dozen rights applicable is that of Subject Access which enables an individual to see/have a copy of the personal data held about them
- carries out Data Protection Impact Assessments (DPIA) where necessary e.g. to ensure protection of personal data when accessed using any remote access solutions, or entering into a relationship with a new supplier
- has undertaken appropriate due diligence and has data protection compliant contracts in place with any data processors
- understands how to share data lawfully and safely with other relevant data controllers.
- has clear and understood policies and routines for the deletion and disposal of data
- reports any relevant breaches to the Information Commissioner within 72hrs of becoming aware of the breach as required by law. It also reports relevant breaches to the individuals affected as required by law. In order to do this, it has a policy for reporting, logging, managing, investigating and learning from information risk incidents
- has a Freedom of Information Policy (Trust policy) which sets out how it will deal with FOI requests
- provides data protection training for all staff at induction and appropriate refresher training thereafter. Staff undertaking particular data protection functions, such as handling requests under the individual's rights, will receive training appropriate for their function as well as the core training provided to all staff

When personal data is stored on any mobile device or removable media the:
- data will be encrypted, and password protected
- device will be password protected
- device will be protected by up-to-date endpoint (anti-virus) software
- data will be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete

Staff must ensure that they:

- always take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse
- can recognise a possible breach, understand the need for urgency and know who to report it to within the school
- can help data subjects understand their rights and know how to handle a request whether verbal or written and know who to pass it to in the school
- only use encrypted data storage for personal data
- will not transfer any school personal data to personal devices
- use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data
- transfer data using encryption, a secure email account (where appropriate), and secure password protected devices

Outcomes

The impact of the Online Safety Policy and practice is regularly evaluated through the review/audit of online safety incident logs; behaviour/bullying reports; surveys of staff, learners; parents/carers and is reported to relevant groups:

- there is balanced professional debate about the evidence taken from the reviews/audits and the impact of preventative work e.g., online safety education, awareness, and training
- there are well-established routes to regularly report patterns of online safety incidents and outcomes to school leadership and governors
- parents/carers are informed of patterns of online safety incidents as part of the school's online safety awareness raising
- online safety (and related) policies and procedures are regularly updated in response to the evidence gathered from these reviews/audits/professional debate
- the evidence of impact is shared with other schools, agencies and LAs to help ensure the development of a consistent and effective local online safety strategy.

School Online Safety Policy Appendices

Appendices

Acceptable Use Agreement

Introduction

Digital technologies have become integral to the lives of children and young people, both within and outside schools. These technologies are powerful tools, which open-up new opportunities for everyone. They can stimulate discussion, encourage creativity, and stimulate awareness of context to promote effective learning. Learners should have an entitlement to safe access to these digital technologies.

This acceptable use agreement is intended:

- to ensure that learners will have good access to devices and online content, be responsible users and stay safe while using digital technologies for educational, personal and recreational use

- to help learners understand good online behaviours that they can use in school, but also outside school

- to protect school devices and networks from accidental or deliberate misuse that could put the security of the systems and users at risk.

Appendix 1 (A1): Learner Acceptable Use Agreement – EYFS & KS1

This is how we stay safe when we use computers:

- I will ask a teacher or suitable adult if I want to use the computers/tablets.

- I will only use activities that a teacher or suitable adult has told or allowed me to use.

- I will take care of computers/tablets and other equipment.

- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong.

- I will tell a teacher or suitable adult if I see something that upsets me on the screen.

- I know that if I break the rules, I might not be allowed to use a computer/tablet.

Appendix 2 (A2): Learner Acceptable Use Agreement – KS2

When I use devices, I must behave responsibly to help keep me and other users safe online and to look after the devices.

For my own personal safety:
- I understand that what I do online will be supervised and monitored and that I may not be allowed to use devices in school unless I follow these rules and use them responsibly.
- I will only visit internet sites that adults have told me are safe to visit.
- I will keep my username and password safe and secure and not share it with anyone else.
- I will be aware of "clever never goes" when I am online.
- I will not share personal information about myself or others when online.
- If I arrange to meet people off-line that I have communicated with online, I will do so in a public place and take a trusted adult with me.
- I will immediately tell an adult if I see anything that makes me feel uncomfortable when I see it online.

I will look after the devices I use, so that the school and everyone there can be safe:
- I will handle all the devices carefully and only use them if I have permission.
- I will not try to alter the settings on any devices or try to install any software or programmes.
- I will tell an adult if a device is damaged or if anything else goes wrong.
- I will only use the devices to do things that I am allowed to do.

I will think about how my behaviour online might affect other people:
- When online, I will act as I expect others to act toward me.
- I will not copy anyone else's work or files without their permission.
- I will be polite and responsible when I communicate with others, and I appreciate that others may have different opinions to me.
- I will not take or share images of anyone without their permission.

I know that there are other rules that I need to follow:
- Where work is protected by copyright, I will not try to download copies (including music and videos).
- When I am using the internet to find information, I should take care to check that the information is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.
- I should have permission if I use the original work of others in my own work.

I understand that I am responsible for my actions, both in and out of school:
- I know that I am expected to follow these rules in school and that I should behave in the same way when out of school as well.
- I understand that if I do not follow these rules, I may be subject to action outlined in the school behaviour policy.

Appendix 3 (A3): Parent/Carer Acceptable Use Agreement

Solent Infant School

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies provide powerful tools, which open new opportunities for everyone. They can stimulate discussion, promote creativity, and stimulate awareness of context to promote effective learning. Young people should always have an entitlement to safe internet access.

This acceptable use policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that parents and carers are aware of the importance of online safety and are involved in the education and guidance of young people with regard to their online behaviour.

The school will try to ensure that learners have good access to digital technologies to enhance their learning and will, in return, expect the learners to agree to be responsible users. A copy of the learner acceptable use agreement is attached to this permission form, so that parents/carers will be aware of the school expectations of the young people in their care.

Parents are requested to sign an electronic permission form within the Arbor App when their child starts at Solent Infant School to show their support of the school in this important aspect of the school's work.

By signing this electronic form within Arbor the parent/carer is confirming that:

I understand that the school has discussed the acceptable use agreement with my son/daughter and that they have received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my son's/daughter's activity on the systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the acceptable use agreement.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's online safety.

As the school is collecting personal data by issuing this form, it will share that:

This form will be stored electronically within the Arbor App.
Staff within the De Curci Trust will have access to this form.
This form will be stored within their child's account within Arbor.
This form will be stored for the length of time their child is at either Solent Infant or Solent Junior School and then passed onto their receiving secondary school. They will then be kept up to 25 years after the child's date of birth.
This form will then be deleted electronically.

Use of Digital/Video Images

The use of digital/video images plays an important part in learning activities. Learners and members of staff may use digital cameras to record evidence of activities in lessons and out of school. These images may then be used in presentations in subsequent lessons.

Images may also be used to celebrate success through their publication in newsletters, on the school website and occasionally in the public media. Where an image is publicly shared by any means, only your child's first name will be used.

The school will comply with the Data Protection Act and request parent's/carer's permission before taking images of members of the school. We will also ensure that when images are published that the young people cannot be identified by the use of their names.

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 in not covered by the Data Protection Act), unless specifically requested not to at an event. 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.

Parents/carers are requested to sign the permission form within the Arbor App when their child starts at Solent Infant School to allow the school to take and use images of their children and for the parents/carers to agree.

As the school is collecting personal data by issuing this form, it will inform parents/carers that:

This form is kept electronically within Arbor	The images
Staff within the De Curci Trust will have access to this form.	The images may be published on; Twitter, Facebook, Instagram, the school's website, local press, and used for marketing purposes.
This form will be stored electronically within Arbor.	Staff from The De Curci Trust will have access to the images.
This form will be passed onto receiving secondary schools and stored up to the child's 25th birthday.	The images will be stored within the schools' network.
This form will be destroyed by deleting it electronically.	The images will be stored until after the year group leaves the school but may be used for historic purposes.
	The images will be destroyed by deleting electronic copies.
	A request for deletion of the images can be made by emailing the request in writing to the Headteacher.

Parents/Carers will be asked to sign a Digital/Video Images Permission Form within the Arbor App when their child starts at Solent Infant School.

Parents/Carers will be asked to sign a 'Use of Cloud Systems' permission form when their child starts at Solent Infant School in order to set up their account on Microsoft 365.

As the school is collecting personal data and sharing this with a third party, it will inform parents/carers that:

This form (electronic or printed)	The data shared with the service provider
Staff within the De Curci Trust will have access to this form.	The data will be shared will be the child's full name.
This form will be stored within Arbor.	The data will be shared with Microsoft.
This form will be passed onto the receiving secondary school and stored until the child's 25th birthday.	Staff within the De Curci Trust will have access to the data.
This form will be deleted electronically.	The data will be stored electronically.
	The data will be stored until the pupil leaves the Solent Schools and then the account will be deleted.
	The data will be destroyed by deleting the account.
	A request for deletion of the data can be made by emailing the Headteacher a request.

Appendix 4 (A4): Staff (and Volunteer) Acceptable Use Policy Agreement

Please see The De Curci Trust Acceptable Use Policy Agreement contained within the IT Operations Handbook.

Related policies

This policy should be read in conjunction with:

- The De Curci Trust – IT Operations Handbook
- The De Curci Trust – AI Policy
- Child Protection and Safeguarding Policy
- Whistleblowing Policy
- Behaviour Policy
- Anti-bullying Policy
- Online safety Policy
- Acceptable Use Agreements
- Curriculum Policies – Teaching and Learning

Appendix 5 (A5): Computer Misuse and Cyber Choices Policy

All key stakeholders, including the school IT service provider, have responsibility for the safeguarding of young people from computer misuse and are aware of the Cyber Choices programme led by the National Crime Agency (NCA) and managed locally by Regional Organised Crime Units (part of the national policing network). The risks to young people of crossing the line into committing cybercrimes is a safeguarding issue.

All staff are made aware of the safeguarding risks of computer misuse.

All staff are familiar with the NCA Hacking it Legal Leaflet*, which explains Cyber Choices and the Computer Misuse Act 1990, and lists recommended resources for teachers to use.

Staff are aware of the role of their local Regional Organised Crime Unit as their point of contact for Cyber Choices referrals.

Learners agree to the Acceptable Use Policy (AUP) which outlines acceptable online behaviours and explains that some online activity is illegal. Acceptable computer use is reinforced across the curriculum, with opportunities to discuss how to act within moral and legal boundaries online, with reference to the Computer Misuse Act 1990.

Any breach of the AUP or activity by a learner that may constitute a cybercrime, in school or at home, will be referred to the Designated Safeguarding Lead for consideration as a safeguarding risk.

Where the DSL believes that the learner may be at risk of committing cybercrimes, or to already be committing cybercrimes, a referral to the local Cyber Choices programme will be made. Where the DSL is unsure if a learner meets the referral criteria, advice should be sought from the local Cyber Choices team.

Parents also have the opportunity report potential cybercrime directly to the local Cyber Choices team but are recommended to make school-based concerns through the DSL.

The IT service provider is aware of the safeguarding requirement to refer concerns about computer misuse to the Designated Safeguarding Lead and has a clear process to follow to do so.

Information for parents about NCA Cyber Choices is available on the school website.

Appendix 6 (A6): Responding to incidents of misuse – flow chart

```
                            ┌─────────────────────────┐
                            │  Online Safety Incident  │
                            └─────────────────────────┘
                ┌───────────────────────┴───────────────────────┐
                ▼                                                ▼
    ┌───────────────────────┐                        ┌───────────────────────┐
    │  Unsuitable materials │                        │   Illegal materials   │
    └───────────────────────┘                        │  or activities found  │
                │                                     │     or suspected      │
                ▼                                     └───────────────────────┘
    ┌───────────────────────┐                                    │
    │   Report to the person│                                    ▼
    │   responsible for     │              ┌─────────────────────────────────────┐
    │   Online Safety       │              │  Report to Police using any number   │
    └───────────────────────┘              │  and report under local safeguarding │
                │                          │           arrangements.              │
                ▼                          │                                      │
    ┌───────────────────────┐              │  DO NOT DELAY, if you have any        │
    │  If staff/volunteer or│              │  concerns, report them immediately.  │
    │  child/young person,  │              └─────────────────────────────────────┘
    │  review the incident  │                        ┌──────────┴──────────┐
    │  and decide upon the  │                        ▼                     ▼
    │  appropriate course of│           ┌──────────────────────┐  ┌──────────────┐
    │  action, applying     │           │ Secure and preserve  │  │     Call     │
    │  sanctions where      │           │      evidence.       │  │ professional │
    │  necessary            │           │                      │  │   strategy   │
    └───────────────────────┘           │ Remember do not      │  │   meeting    │
          ┌──────┴──────┐               │ investigate yourself.│  └──────────────┘
          ▼             ▼               │ Do not view or take  │
 ┌─────────────┐ ┌─────────────┐        │ possession of any    │
 │ Debrief on  │ │Record details│       │ images/videos. Do    │
 │online safety│ │in incident   │       └──────────────────────┘
 │ incident    │ │ log          │                    │
 └─────────────┘ └─────────────┘                     ▼
        │             │              ┌──────────────────────┐
        ▼             ▼              │    Await Police       │
 ┌─────────────┐ ┌─────────────┐     │     response          │
 │Review polices│ │Provide collated│  └──────────────────────┘
 │and share    │ │incident report │   ┌────────┴────────┐
 │experiences  │ │logs to relevant│   ▼                 ▼
 │and practice │ │authority as    │ ┌──────────────┐ ┌──────────────┐
 │as required. │ │appropriate     │ │If no illegal │ │If illegal    │
 └─────────────┘ └─────────────┘   │activity or   │ │activity or   │
        │                          │material is   │ │materials are │
        ▼                          │confirmed,    │ │confirmed,    │
 ┌─────────────┐                   │then revert to│ │allow Police  │
 │ Implement   │                   │internal      │ │or relevant   │
 │ changes     │                   │procedures.   │ │authority to  │
 └─────────────┘                   └──────────────┘ │complete their│
        │                                           │investigation │
        ▼                                           │and seek      │
 ┌─────────────┐                                    │advice from   │
 │  Monitor    │                                    │the relevant  │
 │  situation  │                                    │professional  │
 └─────────────┘                                    │body          │
                                                    └──────────────┘
 ┌───────────────────────────┐     ┌───────────────────────────────────┐
 │ Named Person is responsible│    │ In the case of a member of staff   │
 │ for the child's wellbeing  │    │ or volunteer, it is likely that a  │
 │ and as such should be      │    │ suspension will take place at the  │
 │ informed of anything that  │    │ point of referral to police,       │
 │ places the child at risk.  │    │ whilst police and internal         │
 │ BUT safeguarding procedures│    │ procedures are being undertaken.   │
 │ must be followed where     │    └───────────────────────────────────┘
 │ appropriate.               │
 └───────────────────────────┘
```

Appendix 7 (A7): Record of reviewing devices/internet sites (responding to incidents of misuse)

Group:
Date:
Reason for investigation:

Details of first reviewing person
Name:
Position:
Signature:

Details of second reviewing person
Name:
Position:
Signature:

Name and location of computer used for review (for web sites)

Website(s) address/device	Reason for concern
Conclusion and Action proposed or taken	

Appendix 8 (A8): Reporting Log

A8 Reporting Log Group:						
Date	**Time**	**Incident**	**Action Taken**		**Incident Reported By**	**Signature**
			What?	**By Whom?**		

Appendix B1: Training Needs Audit Log

B1 Training Needs Audit Log

Group: ....

Relevant training the last 12 months	Identified Training Need	To be met by	Cost	Review Date

Appendix C1: School Technical Security Policy

Please also see The De Curci Trust 'Trust IT Operations Handbook for additional technical security policies.

Including:
- Information Security Policy
- AI Policy
- Patch Management Policy
- Anti-Malware Policy
- Access Control Policy
- Password Policy
- Secure Configuration Policy
- Encryption Policy
- Technical Bring Your Own Device (BYOD) Policy
- Domain Security Policy
- Supply Chain Security Policy
- Personnel; Security Policy
- Ransomware Policy
- IT Asset Disposal Policy
- Firewall Policy
- IT Acceptable Use Policy (Staff and Volunteers)

Introduction

Effective technical security depends not only on technical measures, but also on appropriate policies and procedures and on good user education and training. This is informed by the Department for Education (DfE) guidance, Keeping Children Safe in Education, and the Digital and Technology Standards and therefore applicable for schools and colleges in England. For schools and colleges outside England, this would be considered good practice, the school should also ensure that they remain compliant with national, local authority or MAT guidance, as relevant. The school is responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that:

- users can only access data to which they have right of access
- access to personal data is securely controlled in line with the school's personal data policy
- system logs are maintained and reviewed to monitor user activity
- there is effective guidance and training for users
- there are regular reviews and audits of the safety and security of school computer systems, including filtering and monitoring provision

This policy is not designed to reproduce the entirety of the DfE's standards but is designed to support governors and senior leaders in the production of a technical security policy. Governors and senior leaders remain responsible for the school's technical security. Responsibilities

Education settings are directly responsible for ensuring they have the appropriate level of security protection procedures in place in order to safeguard their systems, staff and learners and review the effectiveness of these procedures periodically to keep up with evolving cyber-crime technologies. The management of technical security is the responsibility of Governors and Senior Leaders, supported in this by the Designated Safeguarding Lead, Online Safety Lead and IT Service Provider.

Policy statements

The school is responsible for ensuring that their infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy and The De Curci Trust Operations Handbook are implemented. It will also need to ensure that the relevant people receive guidance and training and will be effective in carrying out their responsibilities: Please see De Curci Trust Operations Handbook for further details.

Filtering and Monitoring

Introduction to Filtering

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so, as online content changes dynamically and new technologies are constantly being developed. It is important, therefore, to understand that filtering is only one element in a larger strategy for online safety and acceptable use. It is important that the school has a filtering policy to manage the associated risks and to provide preventative measures which are relevant to the situation in this school. Many users are not aware of the flexibility provided by many filtering services at a local level for schools. Where available, schools should use this flexibility to meet their learning needs and reduce some of the frustrations occasionally felt by users who wish to maximise the use of the new technologies. Provide training and awareness raising to help users understand the process that is available to them.

Our school filtering system is operational, up to date and applied to all:
- users, including guest accounts.
- school owned devices
- devices using the school broadband connection.

Our filtering system:
- filters all internet feeds, including any backup connections.
- be age and ability appropriate for the users and be suitable for educational settings.

- handle multilingual web content, images, common misspellings and abbreviations.
- identify technologies and techniques that allow users to get around the filtering such as VPNs and proxy services and block them.
- provide alerts when any web content has been blocked.

Mobile and app content is often presented in a different way to web browser content. If your users access content in this way, you should get confirmation from your provider as to whether they can provide filtering on mobile or app technologies. A technical monitoring system should be applied to devices using mobile or app content to reduce the risk of harm.

Introduction to Monitoring

Monitoring user activity on school and college devices is an important part of providing a safe environment for children and staff. Unlike filtering, it does not stop users from accessing material through internet searches or software. Monitoring allows you to review user activity on school and college devices. For monitoring to be effective it must pick up incidents urgently, usually through alerts or observations, allowing you to take prompt action and record the outcome.

Your monitoring strategy should be informed by the filtering and monitoring review. A variety of monitoring strategies may be required to minimise safeguarding risks on internet connected devices and may include:

- physically monitoring by staff watching screens of users
- live supervision by staff on a console with device management software
- network monitoring using log files of internet traffic and web access
- individual device monitoring through software or third-party services

DfE Keeping Children Safe in Education requires schools to have "appropriate monitoring". DfE published Filtering and monitoring standards for schools and colleges in March 2023. Schools are recommended to use the UK Safer Internet Centre Definitions to help them determine if their monitoring system is appropriate to help them determine if their monitoring system is appropriate

Filtering and Monitoring Responsibilities

DfE Filtering Standards require that schools and colleges identify and assign roles and responsibilities to manage your filtering and monitoring systems, and include

Role	Responsibility	Name / Position
Responsible Governor	Strategic responsibility for filtering and monitoring and need assurance that the standards are being met.	
Senior Leadership	Team Member Responsible for ensuring these standards are met and: • procuring filtering and monitoring systems • documenting decisions on what is blocked or allowed and why • reviewing the effectiveness of your provision • overseeing reports Ensure that all staff: • understand their role • are appropriately trained • follow policies, processes and procedures • act on reports and concerns	
Designated Safeguarding Lead	Lead responsibility for safeguarding and online safety, which could include overseeing and acting on: • filtering and monitoring reports • safeguarding concerns • checks to filtering and monitoring systems	
IT Service Provider	Technical responsibility for: • maintaining filtering and monitoring systems • providing filtering and monitoring reports • completing actions following concerns or checks to systems	
All staff need to be aware of reporting mechanisms for safeguarding and technical concerns. They should report if:	• they witness or suspect unsuitable material has been accessed • they can access unsuitable material • they are teaching topics which could create unusual activity on the filtering logs • there is failure in the software or abuse of the system • there are perceived unreasonable restrictions that affect teaching and learning or administrative tasks • they notice abbreviations or misspellings that allow access to restricted material	

Policy Statements

Internet access is filtered for all users. Differentiated internet access is available for staff and customised filtering changes are managed by the school. Illegal content is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation URL list and other illegal content lists. Filter content lists are regularly updated, and internet use is logged and frequently monitored. The monitoring process alerts the school to breaches of the filtering policy, which are then acted upon. There is a clear route for reporting and managing changes to the filtering system. Where personal mobile devices are allowed internet access through the school network, filtering will be applied that is consistent with school practice.

- There is a filtering and monitoring system in place that safeguards staff and learners by blocking harmful, illegal and inappropriate content.
- There is a monitoring system that enables the prompt investigation of a potential safeguarding incident and outcomes are logged.
- Roles and responsibilities for the management of filtering and monitoring systems have been defined and allocated.
- The filtering and monitoring provision is reviewed at least annually and checked regularly.
- There is a defined and agreed process for making changes to the filtering or monitoring system that involves a senior leader in the agreement of the change.
- Mobile devices that access the school's internet connection (whether school or personal devices) will be subject to the same filtering standards as other devices on the school systems.
- The school has provided enhanced/differentiated user-level filtering through the use of the Net Sweeper filtering system (allowing different filtering levels for different ages/stages and different groups of users – staff/learners etc.)

Changes to Filtering and Monitoring Systems

There is a clear process for requests to change the filtering and monitoring systems.
- Users may request changes to the filtering and monitoring systems by emailing the Network Manager and Designated Safeguarding Lead directly.
- It is only with the authorisation from the Designated Safeguarding Lead that changes can be made.
- Changes will only be made where the Designated Safeguarding Lead believes that the change would be of educational value with low risk associated.
- A log of requests and changes is kept by the Designated Safeguarding Lead using email systems.

Filtering and Monitoring Review and Checks

To understand and evaluate the changing needs and potential risks of the school, the filtering and monitoring provision will be reviewed at least annually. The review will be conducted by members of the senior leadership team, the designated safeguarding lead (DSL), and the IT service provider. Additional checks to filtering and monitoring will be informed by the review process so

that governors have assurance that systems are working effectively and meeting safeguarding obligations.

Reviewing the filtering and monitoring provision

A review of filtering and monitoring will be carried out to identify the current provision, any gaps, and the specific needs of learners and staff.

The review will take account of:
- the risk profile of learners, including their age range, pupils with special educational needs and disability (SEND), pupils with English as an additional language (EAL)
- what the filtering system currently blocks or allows and why
- any outside safeguarding influences, such as county lines
- any relevant safeguarding reports
- the digital resilience of learners
- teaching requirements, for example, the RHSE and PSHE curriculum
- the specific use of chosen technologies, including Bring Your Own Device (BYOD)
- what related safeguarding or technology policies are in place
- what checks are currently taking place and how resulting actions are handled

To make the filtering and monitoring provision effective, the review will inform:
- related safeguarding or technology policies and procedures
- roles and responsibilities
- training of staff
- curriculum and learning opportunities
- procurement decisions
- how often and what is checked
- monitoring strategies

The review will be carried out as a minimum annually, or when:
- a safeguarding risk is identified
- there is a change in working practice, e.g. remote access or BYOD
- new technology is introduced

Checking the filtering and monitoring systems

Checks to filtering and monitoring systems are completed and recorded as part of the filtering and monitoring review process. How often the checks take place will be based on the context, the risks highlighted in the filtering and monitoring review, and any other risk assessments. Checks will be undertaken from both a safeguarding and IT perspective.

When filtering and monitoring systems are checked this should include further checks to verify that the system setup has not changed or been deactivated. Checks are performed on a range of:

- school owned devices and services, including those used off site
- geographical areas across the site
- user groups, for example, teachers, pupils and guests

Logs of checks are kept so they can be reviewed. These record:

- when the checks took place
- who did the check
- what was tested or checked
- resulting actions

The school uses the SWGfL Filtering Standards checklist to help with this.

Training/Awareness

It is a statutory requirement in England that staff receive training, at least annually, about safeguarding, child protection, online safety and filtering and monitoring. Furthermore, in order to protect personal and sensitive data, governors, senior leaders, staff and learners should receive training about information security and data protection, at least annually.

Governors, Senior Leaders and staff are made aware of the expectations of them:

- at induction
- at whole-staff/governor training
- through the awareness of policy requirements
- through the acceptable use agreements
- in regular updates throughout the year

Those with specific responsibilities for filtering and monitoring (Responsible Governor, DSL, OSL or other relevant persons) will receive enhanced training to help them understand filtering and monitoring systems and their implementation and review.

Learners are made aware of the expectations of them:

- in lessons (the schools should describe how this will take place)
- through the acceptable use agreements

Parents will be informed of the school's filtering policy through the acceptable use agreement and through online safety awareness sessions and the school newsletter.

Audit/Monitoring/Reporting/Review

Governors/SLT/DSL/OSL will ensure that full records are kept of:

- Training provided
- User Ids and requests for password changes
- User logons
- Security incidents related to this policy
- Annual online safety reviews including filtering and monitoring
- Changes to the filtering system
- Checks on the filtering and monitoring systems

Further Guidance

Schools in England (and Wales) are required *"to ensure children are safe from terrorist and extremist material when accessing the internet in school, including by establishing appropriate levels of filtering"*. Furthermore, the Department for Education's statutory guidance 'Keeping Children Safe in Education' obliges schools and colleges in England to "*ensure appropriate filters and appropriate monitoring systems are in place and regularly review their effectiveness*" and they "*should be doing all that they reasonably can to limit children's exposure to the above risks from the school's or college's IT system*" however, schools will need to "*be careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding.*" Ofsted concluded as far back as 2010 that "*Pupils in the schools that had 'managed' systems had better knowledge and understanding of how to stay safe than those in schools with 'locked down' systems. Pupils were more vulnerable overall when schools used locked down systems because they were not given enough opportunities to learn how to assess and manage risk for themselves.*"

To further support schools and colleges in England, the Department for Education published Digital and Technology standards.

The UK Safer Internet Centre has produced guidance on "Appropriate Filtering and Monitoring"

SWGfL, on behalf of UK Safer Internet Centre and DfE, developed further Filtering and Monitoring | SWGfL information for schools and colleges, including a checklist alongside further support for Governors

SWGfL provides a site for schools to test their filtering to ensure that illegal materials cannot be accessed: SWGfL Test Filtering

Appendix C2: Mobile Technologies Policy (including BYOD/BYOT)

Please see The De Curci Trust IT Operations Handbook for the trust mobile technologies policy including BYOD.

Appendix C3: Social Media Policy

Social media (e.g. Facebook, Twitter, LinkedIn) is a broad term for any kind of online platform which enables people to directly interact with each other. However, some games, for example Minecraft or World of Warcraft and video sharing platforms such as You Tube have social media elements to them.

The school recognises the numerous benefits and opportunities which a social media presence offers. Staff, parents/carers and learners are actively encouraged to find creative ways to use social media. However, there are some risks associated with social media use, especially around the issues of safeguarding, bullying and personal reputation. This policy aims to encourage the safe use of social media by the school, its staff, parents, carers and children.

Scope

This policy is subject to the school's codes of conduct and acceptable use agreements.

This policy:

- Applies to all staff and to all online communications which directly or indirectly, represent the school.
- Applies to such online communications posted at any time and from anywhere.
- Encourages the safe and responsible use of social media through training and education.
- Defines the monitoring of public social media activity pertaining to the school.

The school respects privacy and understands that staff and learners may use social media forums in their private lives. However, personal communications likely to have a negative impact on professional standards and/or the school's reputation are within the scope of this policy.

Professional communications are those made through official channels, posted on a school account or using the school name. All professional communications are within the scope of this policy.

Personal communications are those made via personal social media accounts. In all cases, where a personal account is used which associates itself with, or impacts on, the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy.

Personal communications which do not refer to or impact upon the school are outside the scope of this policy.

Digital communications with learners are also considered. Staff may use social media to communicate with learners via a school social media account for teaching and learning purposes but must consider whether this is appropriate and consider the potential implications.

Organisational control

Roles & Responsibilities

SLT
- Facilitating training and guidance on Social Media use.
- Developing and implementing the Social Media policy.
- Taking a lead role in investigating any reported incidents.
- Making an initial assessment when an incident is reported and involving appropriate staff and external agencies as required.
- Receive completed applications for Social Media accounts.
- Approve account creation.

Administrator/Moderator
- Create the account following SLT approval.
- Store account details, including passwords securely.
- Be involved in monitoring and contributing to the account.
- Control the process for managing an account after the lead staff member has left the organisation (closing or transferring).

Staff
- Know the contents of and ensure that any use of social media is carried out in line with this and other relevant policies.
- Attending appropriate training.
- Regularly monitoring, updating and managing content he/she has posted via school accounts.
- Adding an appropriate disclaimer to personal accounts when naming the school.

Process for creating new accounts

The school community is encouraged to consider if a social media account will help them in their work, e.g. an Early Years Twitter account, or a "New Entrants" Facebook page. Anyone wishing to create such an account must present a business case to the Leadership Team which covers the following points:-

- The aim of the account.
- The intended audience.
- How the account will be promoted.
- Who will run the account (at least two staff members should be named).
- Will the account be open or private/closed.

Following consideration by the SLT an application will be approved or rejected. In all cases, the SLT must be satisfied that anyone running a social media account on behalf of the school has read and understood this policy and received appropriate training. This also applies to anyone who is not directly employed by the school, including volunteers or parents.

Monitoring

School accounts must be monitored regularly and frequently (preferably 7 days a week, including during holidays). Any comments, queries or complaints made through those accounts must be responded to within 48 hours (or two working days even if the response is only to acknowledge receipt. Regular monitoring and intervention is essential in case a situation arises where bullying or any other inappropriate behaviour arises on a school social media account.

Behaviour

- The school requires that all users using social media adhere to the standard of behaviour as set out in this policy and other relevant policies.
- Digital communications by staff must be professional and respectful at all times and in accordance with this policy. Staff will not use social media to infringe on the rights and privacy of others or make ill-considered comments or judgments about staff. School social media accounts must not be used for personal gain. Staff must ensure that confidentiality is maintained on social media even after they leave the employment of the school.
- If a journalist makes contact about posts made using social media staff must follow the trust media policy before responding.
- Unacceptable conduct, (e.g. defamatory, discriminatory, offensive, harassing content or a breach of data protection, confidentiality, copyright) will be considered extremely seriously by the school and will be reported as soon as possible to a relevant senior member of staff and escalated where appropriate.
- The use of social media by staff while at work may be monitored, in line with school policies. The school permits reasonable and appropriate access to private social media sites whilst on breaks and only in adult only spaces where pupils are not present. However, where excessive use is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken.
- The school will take appropriate action in the event of breaches of the social media policy. Where conduct is found to be unacceptable, the school will deal with the matter internally. Where conduct is considered illegal, the school will report the matter to the police and other relevant external agencies and may take action according to the disciplinary policy.

Legal considerations

- Users of social media should consider the copyright of the content they are sharing and, where necessary, should seek permission from the copyright holder before sharing.
- Users must ensure that their use of social media does not infringe upon relevant data protection laws, or breach confidentiality.

Handling abuse

- When acting on behalf of the school, respond to harmful and / or offensive comments swiftly and with sensitivity.
- If a conversation turns and becomes offensive or unacceptable, school users should block, report or delete other users or their comments/posts and should inform the audience exactly why the action was taken.
- If you feel that you or someone else is subject to abuse by colleagues through use of online communications, then this action must be reported using the agreed school protocols.

Use of images

School use of images can be assumed to be acceptable, providing the following guidelines are strictly adhered to.

- Permission to use any photos or video recordings should be sought in line with the school's digital and video images policy. If anyone, for any reason, asks not to be filmed or photographed then their wishes should be respected.
- Under no circumstances should staff share or upload learner pictures online other than via official school channels.
- Staff should exercise their professional judgement about whether an image is appropriate to share on school social media accounts. Learners should be appropriately dressed, not be subject to ridicule and must not be on any school list of children whose images must not be published.
- If a member of staff inadvertently takes a compromising picture which could be misconstrued or misused, they must delete it immediately.

Personal use

Staff

- Personal communications are those made via a personal online account. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy.
- Personal communications which do not refer to or impact upon the school are outside the scope of this policy.

Learners

- Staff are not permitted to follow or engage with current or prior (of less than 18 years of age) learners of the school on any personal social media account.
- The school's education programme should enable the learners to be safe and responsible users of social media.
- Learners are encouraged to comment or post appropriately about the school. Any offensive or inappropriate comments will be resolved by the use of the school's behaviour policy

Parents/Carers

- If parents/carers have access to a school learning platform where posting or commenting is enabled, parents/carers will be informed about acceptable use.
- Parents/Carers are encouraged to comment or post appropriately about the school. In the event of any offensive or inappropriate comments being made, the school will ask the parent/carer to remove the post and invite them to discuss the issues in person. If necessary, refer parents to the school's complaints procedures.

Glossary of Terms

AI	Artificial Intelligence
AUP/AUA	Acceptable Use Policy/Acceptable Use Agreement
BYOD	Bring Your Own Device
BYOT	Bring Your Own Tools (Technology)
CEOP	Child Exploitation and Online Protection Centre (part of National Crime Agency, UK Police, dedicated to protecting children from sexual abuse, providers of the Think U Know programmes.
CPD	Continuous Professional Development
FOSI	Family Online Safety Institute
ICO	Information Commissioners Office
ICT	Information and Communications Technology
INSET	In Service Education and Training
IP address	The label that identifies each computer to other computers using the IP (internet protocol)
ISP	Internet Service Provider
ISPA	Internet Service Providers' Association
IWF	Internet Watch Foundation
LAN	Local Area Network
MAT	Multi Academy Trust
MIS	Management Information System
OS	Online Safety
OSL	Online Safety Lead
TUK	Think U Know – educational online safety programmes for schools, young people and parents.
UKSIC	UK Safer Internet Centre – EU funded centre. Main partners are SWGfL, Childnet and Internet Watch Foundation.
UKCIS	UK Council for Internet Safety
WAP	Wireless Application Protocol