St Augustine's Catholic Primary School

Online Safety Policy

"We love and learn together by growing in friendship with Jesus"

Linked virtues:

'Attentive and Discerning' 'Curious and Active'

September 2025

This policy applies to all members of the school community (including staff, students, volunteers, parents/carers, visitors, community users) who have access to and are users of school ICT systems both in and out of school. The aim of this policy is to ensure that all are aware of the safety issues associated with information systems and electronic communications. Its purpose is to allow all members of our community to enjoy the many benefits of electronic communication whilst understanding the dangers and taking appropriate precautions to keep themselves safe.

The Online Safety Policy relates to other policies including those for Computing, Use of social media, Remote Learning, Mobile Devices Policy and safeguarding. The school will deal with such incidents within this policy and associated behaviour and child protection policies, and will, where known, inform parents/carers of incidents of inappropriate Online Safety behaviour that takes place out of school.

- The online safety co-ordinator is Miss A. Brennan supported by Mrs. J. Foley (Head Teacher & DSL), Miss C. Harwood (Deputy Head Teacher and DSL) and Mr. M. Crooks (Technician)
- Our Online Safety Policy has been written by the school, building on guidance from Solihull Council and resources from the South West Grid for Learning.

This policy aims to promote a whole school approach to online safety by:

- Setting out expectations for all St Augustine's Catholic Primary School community members' online behaviour, attitudes and activities and use of digital technology (including when devices are offline)
- Helping safeguarding and senior leadership teams to have a better understanding and awareness of all elements of online safeguarding through effective collaboration and communication with technical colleagues (e.g. for filtering and monitoring), curriculum leads (e.g. RSHE) and beyond.
- Helping all stakeholders to recognise that online/digital behaviour standards (including social media activity) must be upheld beyond the confines of the school gates and school day, regardless of device or platform, and that the same standards of behaviour apply online and offline.
- Facilitating the safe, responsible, respectful and positive use of technology to support teaching & learning, increase attainment and prepare children and young people for the risks and opportunities of today's and tomorrow's digital world, to survive and thrive online
- Helping school staff working with children to understand their roles and responsibilities to work safely and responsibly with technology and the online world:
    - for the protection and benefit of the children and young people in their care, and
    - for their own protection, minimising misplaced or malicious allegations and to better understand their own standards and practice.
    - for the benefit of the school, supporting the school ethos, aims and objectives, and protecting the reputation of the school and profession.
- Establishing clear structures by which online misdemeanours will be treated, and procedures to follow where there are doubts or concerns (with reference to other school policies such as Behaviour Policy or Anti-Bullying Policy)

Further Help & Support:

Internal school channels should always be followed first for reporting and support, as documented in school policy documents, especially in response to incidents, which should be reported in line with your Child Protection & Safeguarding Policy. The DSL will handle referrals to local authority multi-agency safeguarding hubs (MASH) and DSL will handle referrals to the LA designated officer (LADO).

Beyond this, National College has a list of curated links and supportive videos to external support and helplines for both pupils, parents and staff. Additionally, the Professionals' Online-Safety Helpline from the UK Safer Internet Centre and the NSPCC Report Abuse Helpline for sexual harassment or abuse, as well as hotlines for hate crime, terrorism and fraud which might be useful to share with parents, and anonymous support for children and young people.

Online Safety Curriculum:

We follow Project Evolve's '*Education for a Connected World*' to ensure we are meeting the objectives on Online Safety as outlined by the DfE. The education of pupils in online safety is an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

Online safety should be a focus in all areas of the curriculum (including RSE and PSHE) and staff should reinforce online safety messages across the curriculum. The online safety curriculum is broad, relevant and provides progression, with opportunities for creative activities and will be provided in the following ways.

Purpose and Intent of Project Evolve: Education for a Connected World

The Project Evolve framework aims to provide a comprehensive and evolving approach to online safety education. It is designed to:

- Equip Children and Young People: help them develop the knowledge, skills, and understanding needed to navigate the online world safely and responsibly.
- Align with DfE Objectives: Ensure that the online safety education aligns with the Department for Education's objectives and statutory requirements.
- Encourage Reflection and Positive Outcomes: move beyond simply telling children what to do or not to do online. Instead, it encourages reflection, critical thinking, and positive behaviour through engaging and meaningful activities.
- Provide Comprehensive Resources: offer a wide range of resources, including perspectives, research, activities, outcomes, supporting materials, and professional development tools for educators.
- Support Continuous Learning: dapt to the changing digital landscape by providing up-to-date and relevant content that addresses current online safety challenges and opportunities

Online Safety in our Curriculum:

- Online safety education through the follow Project Evolve '*Education for a Connected World*' curriculum, and through the use of 'Be Internet Legends' resources (particularly in Key Stage Two).
- Please refer to Appendix 5 for more information regarding the Be Internet Legends Online Safety pillars.
- Pupils should be taught in all lessons to be critically aware of the materials and content they access online and be guided to validate the accuracy of this information.
- Pupils will be taught about acceptable Internet use and which Internet use is acceptable and given clear objectives for Internet use, including the use of AI.
- Pupils will understand that their use will be monitored and can be traced back to the user through their username.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Pupils should be supported in building resilience to radicalisation.
- Pupils should be taught about the safe and appropriate use of mobile technologies, and as a staff we must strive to keep up to date with new technologies.
- Pupils should be helped to understand the need for the pupil Acceptable use agreement and encouraged to adopt safe and responsible use both within and outside school.
- Safer Internet Day (February each year) will be an active source of Teaching & Learning.
- Be Internet Legends and SMART rules posters are posted around the school/in each classroom and are referred to in lessons.
- Pupils are advised never to give out personal details of any kind which may identify them or their location. Examples would include real name, address, mobile or landline phone numbers, school, IM address, email address, names of friends, specific interests and clubs etc.
- Pupils will be encouraged not to use Social Networking sites until they are legally old enough.

If staff or pupils discover unsuitable sites or content this must be reported to the Head Teacher who will report it to the SMBC EICTS (Education ICT services) team. This is alongside the use of our filtering/monitoring system (Smoothwall).

Responsibilities – Headteacher and Senior Leaders

- The headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community and fostering a culture of safeguarding, though the day-to-day responsibility for online safety is held by the Designated Safeguarding Lead, as defined in Keeping Children Safe in Education.
- The headteacher 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 .
- The headteacher/senior leaders are responsible for ensuring that the Designated Safeguarding Lead / Online Safety Lead, IT provider 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 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 headteacher/senior leaders will receive regular monitoring reports from the Designated Safeguarding Lead / Online Safety Lead.
- The headteacher/senior leaders will work with the responsible Governor, the designated safeguarding lead (DSL) and IT service providers in all aspects of filtering and monitoring.

Responsibilities – Governing Body

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 Governing body, 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)
- 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 IT service provider and involve the responsible governor) - in-line with the DfE Filtering and Monitoring Standards
- reporting to relevant governors meeting
- Receiving 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

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

Responsibilities – The 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"
While the responsibility for online safety is held by the DSL and cannot be delegated, St Augustine's does have an Online Safety Leader, who works directly alongside the DSL.

The DSL will:

- co-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 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 IT providers on matters of safety and safeguarding and welfare (including online and digital safety)

The DSL will work alongside the OSL, whose responsibilities are:

Online Safety Lead

The Online Safety Lead will:

- lead the Online Safety Group
- work closely on a day-to-day basis with the Designated Safeguarding Lead (DSL),
- 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
- promote an awareness of and commitment to online safety education, 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) with regard to the areas defined In Keeping Children Safe in Education:
  - content
  - contact
  - conduct
  - commerce

Responsibilities – Curriculum Lead

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

This will be provided through:

- PHSE and SRE programmes
- A mapped cross-curricular programme
- assemblies and pastoral programmes
- through relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week.

Responsibilities - 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 staff acceptable use agreement (AUA)
- they immediately report any suspected misuse or problem to Mrs J Foley 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
- 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 video-conferencing, there is regard to national safeguarding guidance and local safeguarding policies
- there is a zero-tolerance approach to incidents of online-bullying, sexual harassment, discrimination, hatred.
- 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.

Students/Pupils 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/carers

Play a crucial role in ensuring that their children understand the need to use the internet and mobile devices in an appropriate way so we also ask parents to sign the 'Pupil Acceptable Use policy' (Appendix 1) alongside their child. The school will take every opportunity to help parents understand these issues through newsletters, letters, website links, parent workshops and information about national campaigns. Parents and carers will be encouraged to support the school in promoting good online safety practice, and to follow guidelines on the appropriate use of digital and video images taken at school events. For Safeguarding purposes, parents/carers **are not allowed to upload** photographs or videos that they take of any school event onto the internet (Twitter/Facebook etc.). They are explicitly reminded about this at school events e.g. assemblies, productions etc. in order to comply with our Safeguarding arrangements. We thank our parents/carers for their cooperation with this matter.

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 (the school will need to decide if they wish parents/carers to acknowledge these by signature)
- publish information about appropriate use of social media relating to posts concerning the school.
- seeking their permissions concerning digital images, cloud services etc (see parent/carer AUA in the appendix)
- parents'/carers' evenings, newsletters, website, social media and information about national/local online safety campaigns and literature.

Authorising Internet Access

- All staff and pupils are granted Internet access, although access could be denied in the event of inappropriate use.
- In the Early Years Foundation Stage pupils are only able to access the sites and software specifically designed for their needs under staff supervision.
- At Key Stage 1 & 2, access to the Internet and Extranet will be by adult demonstration with directly supervised access to specific, approved on-line materials (safe searches).

Assessing risks

The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor SMBC can accept liability for the material accessed, or any consequences of Internet access.

E-Mail

- Pupils may only use approved email accounts on the school system.
- Pupils must immediately tell a teacher if they receive an offensive email.
- Pupils must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission.
- Pupils must only email people teachers/school has approved
- Emails sent must always be polite and friendly.
- Email sent to an external organisation will be written carefully and authorised before sending, in the same way as a letter written on school headed paper. Pupils must not open emails from people they don't know.
- The forwarding of chain letters is not permitted.
- Staff at this school use the email system provided by Microsoft Office - Outlook for all school emails. They never use a personal/private email account (or other messaging platform) to communicate with children or parents, or to colleagues when relating to school/child data, using a non-school-administered system.

Use of digital and video images

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular, they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Written permission from parents/carers will be obtained before photographs of pupils are published on the school website/social media/local press. Each academic year a reminder regarding this consent will be in the school newsletter, and if parents wish to change they must inform us.
- If a child's photograph is not allowed to be published then this information will be put on display in the staff room to ensure information is available to all staff in school.
- 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. To respect everyone's privacy and in some cases protection these images should not be published nor should parents/carers comment on any activities involving other pupils in the digital images.
- Please refer to the Mobile Devices Policy for guidance on appropriate use of both school and personal equipment.
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Pupils work can only be published with the permission of the pupil and parents or carers.

Published content and the school web site

- The contact details on the web site should be the school address, email and telephone number. Staff or pupils personal information will not be published.
- The Head Teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

- The school web site has links to online safety sites for parents.

Managing Videoconferencing

Microsoft Teams is used across the MAC for school meetings and briefings.

Information System Security

- The security of the school information systems will be reviewed regularly.
- Virus protection will be installed and updated regularly (Solihull M.B.C.)
- The school uses the Solihull Broadband with its firewall and filters.

IT Systems:

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 IT Provider 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 (insert relevant person) 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 (see appendix 'Technical Security Policy template' for good practice).
- monitoring systems are implemented and regularly updated as agreed in school policies

Managing filtering and monitoring

- The school will work in partnership with the Solihull EICTS Development Service to ensure filtering and monitoring systems continue to be as effective as possible.
- Senior staff are responsible for ensuring that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- In the academic year 2016-17, filtering and monitoring was updated through our links with Solihull council, and we currently use 'Smoothwall'. This filter system is still in place and working effectively.
- The filtering system automatically checks all content including content that was not previously checked. This supports the '*Keeping Children Safe in Education 2024*' document.
- The monitoring system reports on all internet use, and these reports will identify potential safeguarding issues and behaviour issues – including *potential* misuse by staff – so that these issues can be investigated by school leaders.

- The Head Teacher receives usage reports as a result of this. Any potential misuse detected could be investigated by the school if it was thought to breach the school's policies.

Handling online safety complaints

- Complaints of internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the Head Teacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Please refer to Appendix E for our Online Safety Log that is part of our 'Positive behaviour and discipline policy'.
- Please also refer to Appendix Three with the online safety incidents flow chart.

Data Protection:

Personal data will be recorded, processed, transferred and made available according to the Schools Data Protection Policy (in accordance with the relevant Data Protection laws, including the General Data Protection Regulations)

This Policy was reviewed and agreed by staff: September 2025

Review date: Annually

Appendix One:

Pupil Acceptable Use Policy

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 keep my username and password safe and secure. I will not share it, and I will not try to use anyone else's username and password.
- I will take care of the computer 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 will follow our online safety guidance and rules when using technology.
- I know that if I break the rules I might not be allowed to use a computer/tablet.

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

- I use the school systems and devices.
- I use my own devices in school (When allowed)
- I use my own equipment out of the school in a way that's related to me being a member of this school.

Signed (child): _____

Signed (parent): _____

Appendix Two:

Acceptable Use Policy for staff

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value and use of digital technology for enhancing learning and will ensure that pupils receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

Members of staff should consult the schools Online Safety, Data Protection, Social Media and Mobile Devices policies for further information and clarification

For my professional and personal safety:

- I understand that the school will monitor my use of the school digital technology and communication systems.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email etc.) out of school, and to the transfer of personal data (digital or paper based) out of school.
- I understand that the school digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username or password to anyone else, nor will I try to use anyone else's. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.
- I will report any incidents of concern regarding children's safety to the appropriate person.

I will be professional in my communications and actions when using school ICT systems

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

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school.

- When I use my mobile devices in school (laptops, tablets, phones) I will follow the rules set out in this agreement and the Mobile Devices Policy, in the same way as if I was using school equipment.

Alongside the Online Safety, Social Media, and Mobile Devices Policy, please also note:

- *The mobile phones of all EYFS staff are to be kept in a locker in the staffroom, not in classes.*
- *KS1 + 2 staff must store phones away from children to ensure they are not accessible by children.*
- *Where possible mobile phones should have a password secured keypad.*

- I will not use personal email addresses on the school ICT systems.
- I will not open any hyperlinks in emails or any attachments to emails unless the source is known and trusted.
- I will ensure that my data is regularly backed up, in accordance with school policies.
- I will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others. I will not try to use any programs or software that might allow me to bypass the schools filtering/security systems.

- I will not install programs of any type on a machine, or store programs on a computer, nor will I try to alter computer settings unless I have been given permission.
- I understand that the data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original works of others in my own work.
- Where work is protected by copyright, I will not download or distribute copies (including music/videos)
- I will promote online safety with students in my care and will help them to develop a responsible attitude to system use, communications and publishing in accordance with the curriculum plans.

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

- I understand that this Acceptable Use Policy applies not only to my work and use of school digital technology equipment in school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School Data Protection Policy. Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based protected and restricted data must be held in lockable storage.
- The school may exercise its right to monitor the use of the schools information systems and internet access, to intercept email and to delete inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing of unlawful text, imagery or sound.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action This could include warning, suspension, referral to Governors and or the Local Authority and in the event of illegal activities the involvement of the police

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

Staff name: _____

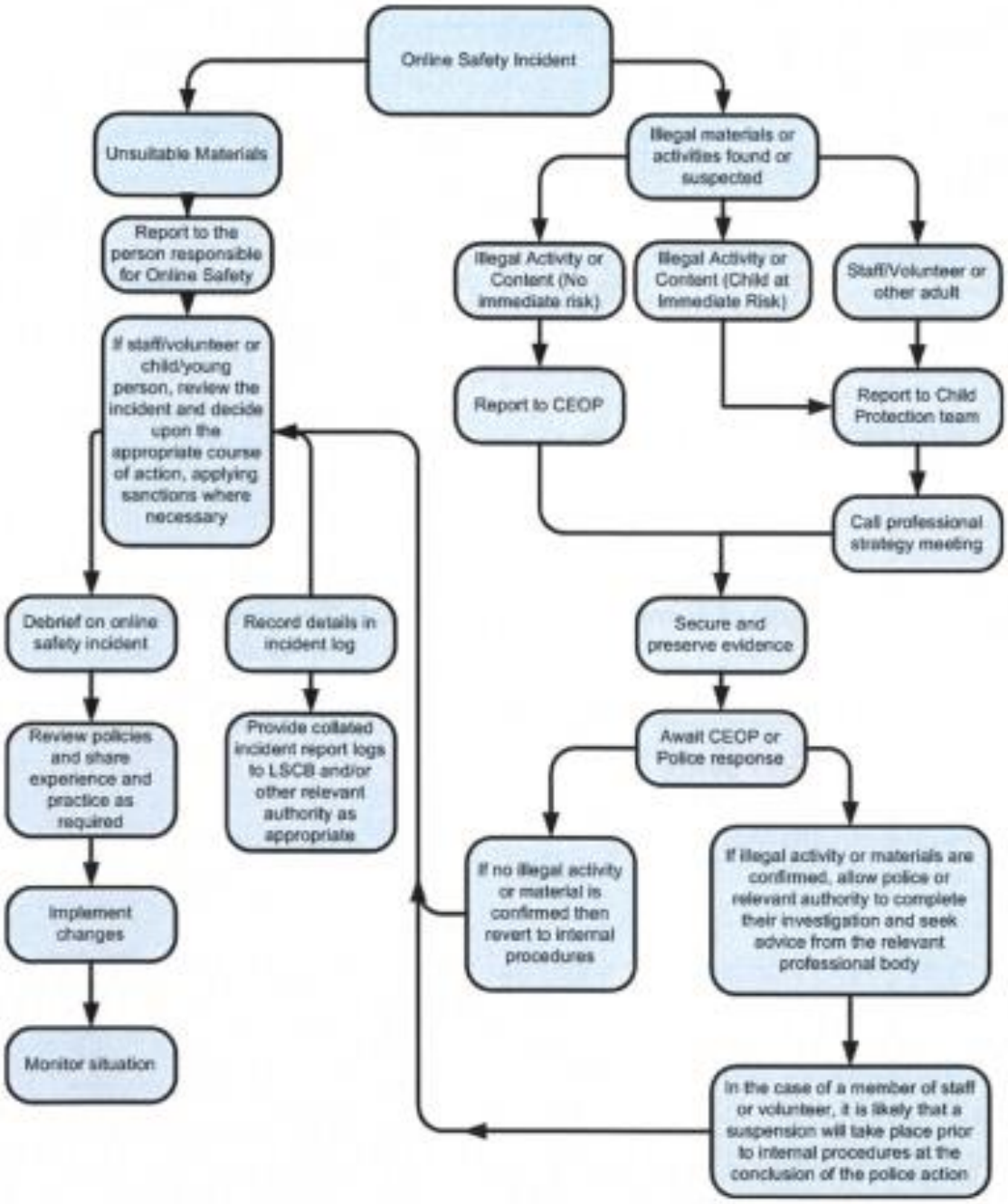
Signed: _____

Date: _____

Appendix Three:

SWGfL Online Safety School / Academy Template Policies

Responding to incidents of misuse – flow chart



Appendix Four:

APPENDIX E

Online Safety Log

* Type of concern: I=Internet; P=Phone; T= Text; L=Letter; D=Discussion

Date	Pupil name	Type of concern	Reason	Follow up

Appendix Five:

Appendix Be Internet Legends – Internet Safety Pillars