



Title	:	Online Safety Policy
File Name	:	WIA/IT-OSP/011-6
Date of Issue	:	1 August 2022
Revision Date	:	20 August 2026
Next Anticipation Date	:	20 August 2027

Online Safety Policy

1. INTRODUCTION

This Online Safety policy considers all current and relevant issues, within the school, linked with other relevant policies, such as the Child Protection / Safeguarding, Behavior, Acceptable Use and Anti- Bullying policies. The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care of all stake holders viz. students, staff, parents, governors. The policy will also form part of the school's protection from legal challenge, relating to the use of digital technologies. The use of the exciting and innovative online tools in school and at home has been shown to raise educational standards and promote pupil / student achievement. However, the use of these new technologies can put users at risk. The breadth of issues within e-safeguarding is considerable, but they can be categorized into three areas of risk:-

Content: being exposed to illegal, inappropriate, or harmful material. Contact: being subjected to harmful online interaction with other users.

Conduct: personal online behavior that increases the likelihood of, or causes, harm.

2. **OBJECTIVE**

To ensure that the whole school has the knowledge to stay safe and risk free whilst online and to ensure that the risks are identified, assessed and mitigated (where possible) in order to reduce the risk of harm to the student or liability to the school. The Online Safety Leader is responsible for reviewing these general e-Safety objectives and setting new ones.

3. **SCOPE**

This policy applies to all members of the school (including staff, students, volunteers, parents / guardian, visitors) who have access to and are users of school ICT systems, both in and out of the school.

4. ROLES AND RESPONSIBILITIES

Online Safety Team

- | | |
|----------------------|----------------------------|
| 1. Ms. Madonna James | Principal (SLT) |
| 2. Ms. Samsheer | Vice Principal (SLT) |
| 3. Ms. Anuja Nair | Online Safety Leader |
| 4. Ms. Rasma | Counsellor |
| 5. Ms. Jeena Jose | IT Staff |
| 6. Ms. Reema Lijo | IT Staff |
| 7. Ms. Malavika | Physical Education Teacher |



- | | |
|-----------------------|---------------------|
| 8. Ms. Mazhar Sultana | E-Monitor (Teacher) |
| 9. Roshan T Benny | E-Monitor(Student) |
| 10. Neveah Manoj | E-Monitor(Student) |

RESPONSIBILITIES

Responsibilities for eSafety are as follows: The Governing Body Is responsible for ensuring that eSafety is implemented and maintained according to this Policy, and for ensuring all necessary resources are available.

- Reads, understands, contributes to and helps promote the school's safeguarding policies and guidance.
- Develops an overview of the benefits and risks of the internet and common technologies used by students.
- Develops an overview of how the school ICT infrastructure provides safe access to the internet. Develops an overview of how the school encourages students to adopt safe and responsible behaviours in their use of technology in and out of school.
- Supports the work of the E-safeguarding group in promoting and ensuring safe and responsible use of technology in and out of school, including encouraging parents to become engaged in E- Safeguarding activities.
- Ensures appropriate funding and resources are available for the school to implement its E-Safeguarding strategy

5. Online Safety Leader

- Takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents.
- Promotes an awareness and commitment to e-safeguarding throughout the school community. Ensures that e-safety education is embedded across the curriculum.
- Communicates with school ICT technical staff.
- Communicates regularly with SLT and the designated E-Safety team / committee to discuss current issues, review incident logs and filtering / change control logs.
- Ensures that all staff are aware of the procedures that need to be followed in the event of an E- Safety incident.
- Ensures that an E-Safety incident log is kept up to date. Facilitates training and advice for all staff.
- Is regularly updated in e-safety issues and legislation, and be aware of the potential for serious child protection issues to arise from:
 - sharing of personal data
 - access to illegal / inappropriate materials
 - inappropriate on-line contact with adults / strangers
 - cyber-bullying and use of social media

Oversees the delivery of the e-safety element of the Computing curriculum. Ensures that appropriate risk assessments are undertaken regarding the safe use of technology. Audit and evaluate online safety practice to identify strengths and areas for improvement. Liaises with the Online Safety team to review policies and



strengthen the e safety measures. Attends training sessions for updating knowledge and skills.

6. Senior Leadership Team:

- The Senior Leadership Team (SLT) has overall responsibility for e-safeguarding all members of the school community, though the day-to-day responsibility for safeguarding will be delegated to the Online Safety Leader (OSL).
- Is responsible for ensuring that the OSL and other relevant staff receive suitable training to enable them to carry out their safeguarding roles and to train other colleagues when necessary.
- Ensures that there is a mechanism in place to allow for monitoring and support of those in school who carry out the internal safeguarding monitoring role. This provision provides a safety net and also supports those colleagues who take on important monitoring roles.
- Receives monitoring reports from the OSL and ensures timely intervention.
- Ensures awareness of procedures to be followed in the event of a serious safeguarding incident. Reviews the e-Safety Policy at least once a year or each time a significant change occurs and prepare minutes from that meeting. The purpose of the management review is to establish the suitability, adequacy, and effectiveness of the e-Safety Policy.

7. IT Staff

- Ensures the school's technical infrastructure is secure as possible and is not open to misuse or malicious attack.
- Ensures that school meets required online safety technical requirements and any Local Authority Guidance that may apply.
- Ensures that users may only access the networks and devices through a properly enforced password protection policy.
- Ensures that the filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person.
- Keeps 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.
- Ensures that use of the network / internet / Learning Platform / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Senior Leadership Team for investigation and possible sanction.
- Monitors software / systems are implemented and updated as agreed in school policies.

8. Teaching and Support Staff

- Should have an up-to-date awareness of online safety matters and of the current school Online Safety Policy and practices.
- understand and adhere to the school staff Acceptable Use Policy. Reports any suspected misuse or problem to the Online Safety Leader.
- develop and maintain an awareness of current safeguarding issues and guidance. Models safe and responsible behaviors in their own use of technology.
- Ensures that any digital communications with pupils should be on a professional level and only through school-based systems, NEVER through personal mechanisms, e.g. personal email ID, text etc.
- Embeds E-Safeguarding messages in learning activities across all areas of the curriculum. Supervises and guide pupils carefully when engaged in learning activities involving technology.
- Ensures that students are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws.



- Is aware of e-Safeguarding issues related to the use of mobile phones, cameras and handheld devices.
- Understands and is aware of incident-reporting mechanisms that exist within the school. Maintains a professional level of conduct in personal use of technology always.
- Ensures that sensitive and personal data is kept secure at all times by using encrypted data storage and by transferring data through secure communication systems.
- Students Read, understand and adhere to the school student Acceptable Use Policy.
- Help and support the school in the creation of safeguarding policies and practices and to adhere to any policies and practices the school creates.
- Know and understand school policies on the use of devices in the school campus.
- Know and understand school policies regarding cyberbullying.
- Take responsibility for learning about the benefits and risks of using the internet and other technologies safely both in school and at home.
- Are fully aware of research skills and of legal issues relating to electronic content such as copyright laws.
- Take responsibility for each other's safe and responsible use of technology in school and at home, including judging the risks posed by the personal technology owned and used outside school.
- Ensure they respect the feelings, rights, values, and intellectual property of others in their use of technology in school and at home.
- Understand what action, they should take if they feel worried, uncomfortable, vulnerable or at risk while using technology in school and at home, or if they know of someone who this is happening to.
- Understand the importance of reporting abuse, misuse, or access to inappropriate materials and to be fully aware of the incident-reporting mechanisms that exists within school.
- Discuss e-Safeguarding issues with family and friends in an open and honest way.
Parents / Guardians.
- Take responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.
- Discuss e Safeguarding concerns with their children, show an interest in how they are using technology and encourage them to behave safely and responsibly when using technology.
- Model safe and responsible behaviours in their own use of technology Consult with the school if they have any concerns about their children's use of technology.
- Agree to and sign the media consent form which clearly sets out the use of photographic and video images of the students.

9. POLICY STATEMENT

Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students in online safety is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognize and avoid online safety risks and build 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 should be provided as part of Computing / PHSE /other lessons and should be regularly revisited.
- online safety messages will be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities.
- Students will be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.



- Students will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Students will be helped to understand the need for the student Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school.
- Staff should act as good role models in their use of digital technologies the internet and mobile devices.
- In lessons where internet use is pre-planned, it is best practice that students 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 students are allowed to freely search the internet, staff should be vigilant in 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 can request that the IT staff (or other relevant designated person) can temporarily remove 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.

10. Education — Parents / Guardians

Many parents and guardians may only have a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring regulation of the children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

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

- Newsletters, web site
- Parents / Guardians awareness sessions
- Reference to the relevant web sites / publications

11. Education & Training — Staff / Volunteers

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. To that end, the following will apply:

- A planned programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced.
- 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 is expected that some staff will identify online safety as a training need within the performance management process. The Online Safety Leader and Online Safety Team will receive regular updates through attendance at external training events.
- Staff will be given the opportunity to discuss the Online Safety Policy and its updates.
- The Online Safety Leader will provide advice / guidance / training to individuals as required.

12. Training — Online Safety Leader



Online Safety Leader should take part in online safety training / awareness sessions, with particular importance for those who are members of the Online Safety Team involved in technology / online safety / health and safety / safeguarding. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority / National Governors Association / or other relevant organization.
- Participation in school training / information session for staff or parents.

13. TECHNICAL - INFRASTRUCTURE /EQUIPMENT, FILTERING. AND MONITORING

It is the responsibility of the school to ensure that the managed service provider carries out all the online safety measures that would otherwise be the responsibility of the school. It is also important that the managed service provider is fully aware of the school Online Safety Policy and Acceptable Use Policy.

The school will be responsible for ensuring that the infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities:

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements.
- There will be regular reviews and audits of the safety and security of school technical systems Servers, wireless systems and cabling must be securely located and physical access restricted All users will have clearly defined access rights to school technical systems and devices.
- All users will be provided with a username and secure password that will be kept up to i.e. name changes etc. Users are responsible for the security of their username and password and will be required to change their password as and when deemed necessary
- The "master / administrator" passwords for the school ICT system, used by the IT administrator services must also be available to the Principal and kept in a secure place The IT staff services is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations.
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband. Content lists are regularly updated and internet use is logged and regularly monitored.
- Internet filtering should ensure that children are safe from terrorist and extremist material when accessing the internet.
- The school has provided enhanced/differentiated user-level filtering (allowing different filtering levels for different ages / stages and different groups of users — staff / students etc.) School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Policy An appropriate system is in place for users to report any actual / potential technical incident / security breach to the relevant person, as agreed.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, workstations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up-to-date virus software.



- An agreed policy is in place regarding the extent of personal use that users are allowed on school devices.
- An agreed policy is in place that allows staff to / forbids staff from downloading executable files and installing programmes on school devices.
- An agreed policy is in place regarding the use of removable media (e.g. memory sticks / CDs/ DVDs) by users on school devices. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

14. MOBILE TECHNOLOGIES (INCLUDING BYOD)

Only mobile technology devices owned by the school has the capability of utilizing the school's wireless network. The device then has access to the wider internet, which may include the school's learning platform and other cloud-based services such as email and data storage. All users should understand that the primary purpose of the use mobile / personal devices in a school context is educational. Teaching about the safe and appropriate use of mobile technologies should be an integral part of the school's Online Safety education programme. Non-school owned mobile devices are not allowed on the school network unless set-up as a guest user who will sign a declaration to abide by the school's internet usage policies. The school Acceptable Use Agreements for staff, students and parents/guardians will give consideration to the use of mobile technologies.

15. USE OF DIGITAL AND VIDEO IMAGES

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / guardians and students need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular, they should recognize the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Written permission from parents or guardians will be obtained before photographs of students are published on the school website / social media / local press.
- Parents / guardians 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 / made publicly available on social networking sites, nor should parents / guardians' comment on any activities involving other students in the digital / video images.
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes care should be taken when taking digital / video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrespect.
- Students must not take, use, share, publish or distribute images of others without their permission. Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images. The school reserves the right to publish student's work produced as part of their education without the permission of the student and parents/ guardians.



16. COMMUNICATIONS

A wide range of rapidly developing communications technologies has the potential to enhance learning.

Communication Technologies	Staff & other adults				Students			
	Allowed	Allowed at certain	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school	Yes						Yes	
Use of mobile phones in lessons		Yes						No
Use of mobile phones in social time	Yes							No
Taking photos on mobile phones or other camera devices	Yes						Yes	
Use of school email for personal emails				No				No
Use of chat rooms / facilities							Yes	
Use of social networking sites				No				No

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

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. must immediately report, to the 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.
- Any digital communication between staff and students or parents (email, social media, chat, etc.) must be professional in tone and content.
- Students should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

17. SOCIAL MEDIA - PROTECTING PROFESSIONAL IDENTITY

All schools and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race, or disability or who defame a third party may render the school or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place. The school does not support the use of social



media accounts and staff should not use social media on school devices and are encouraged not to use social media on their own devices during school hours.

The school pro-actively monitors the internet for public postings about the school and responds to social media comments made by others according to a defined policy or process.

The school's use of social media for professional purposes will be checked regularly by the IT Staff services and Online Safety Team to ensure compliance with the school policies.

18. UNSUITABLE / INAPPROPRIATE ACTIVITIES

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other technical systems. Other activities e.g. cyber- bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities.

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts certain internet usage as follows:

		Acceptable	Acceptable at certain times	Acceptable for certain users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or	Child sexual abuse images					?
	Promotion or conduct of illegal acts, eg under the child protection, obscenity, computer Misuse and fraud legislation					?
	Pornography				?	
	Promotion of any kind of discrimination				?	
	Promotion of racial or religious hatred				?	
	Threatening behavior, including promotion of physical violence or mental				?	
comments that contain or relate to:	Any other information which may be offensive to colleagues or					



	breaches the integrity of the ethos of the school or brings the school into dispute					
Using school systems to run a private business						
Use systems, applications, websites or other mechanisms that b ass the filtering						
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions						
Revealing or publicizing confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)						
Creating or propagating computer viruses or other harmful files						
On-line gaming (non-educational)						
File sharing						
Use of social networking sites						
Use of video broadcasting e.g. YouTube						

19. OTHER INCIDENTS

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary, can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should 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 (except in the case of images of child sexual abuse).
- 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:
 - Intimal response or discipline procedures
 - Involvement by Local Authority or national / local organization (as relevant).
 - Police involvement and/or action

If content being reviewed includes images of Child abuse, then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:



- incidents of 'grooming' behavior of the sending of obscene materials to a child or adult material which potentially breaches the Obscene Publications Act or criminally racist material or promotion of terrorism or extremism or other criminal conduct, activity or materials.
- Isolate the computer and question as best you can. Any change to its state may hinder a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

20. RESPONDING TO INCIDENTS OF MISUSE

It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse:

If any apparent or actual misuse appears to involve illegal activity e.g.

- child sexual abuse images.
- adult material which potentially breaches the Obscene Publications Act.
- criminally racist material.
- Other criminal conduct, activity or materials

If members of staff suspect that misuse might have taken place, but that the misuse is not illegal it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. 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.

Revision

Revision Date	File Name	Revision
1-Oct-2020	WIA/IT-OSP/011	New policy
10 Oct 2021	WIA/IT-OSP/011-1	Change in Committee Members
1 Sept 2022	WIA/IT-OSP/011-2	Change in Committee Members
15- July-2023	WIA/IT-OSP/011-3	Logo Change, Change in committee members
20- Aug- 2024	WIA/IT-OSP/011-4	Change in committee members, change of name of file, policy reviewed
20-Aug-2025	WIA/IT-OSP/011-5	Reviewed and Approver's signature
20-Aug-2026	WIA/IT-OSP/011-6	Reviewed and Approver's signature

Approvals


Principal (Mrs. Madonna James)

