Chiron OEP Online Safety Policy

Policy implemented:	June 2023
Last reviewed:	New Policy
Next review due:	June 2025

1. Summary

This Online Safety Policy outlines the commitment of Chiron OEP to safeguard members of our school community online in accordance with statutory guidance and best practice. This policy is created in accordance with the relevant legislation. Chiron OEP 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.

Safeguarding and protecting the people we support effectively is central to all of Ambito Education's work and supports Ambito Education's strategy to maximise the life opportunities and the health and wellbeing of disabled people. All staff and volunteers recognise that safeguarding is everyone's responsibility irrespective of the role they undertake or whether their role has direct contact or responsibility for our customers or not. This commitment is equally as strong in the virtual spaces as it in when dealing with young people face-to-face.

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 on our internal comms system (Blink)
- *is published on the school website.*

2. Document Control

Initial purpose and scope of the new policy/procedure agreed by:	Ayesha Allen, Virtual School Head
Technical review carried out:	Michael Albero, March 2023
Final quality check carried out:	Luke Laville, June 2023
Date implemented:	June 2023
Version Number:	1.0
Date of the next review:	June 2025
Department responsible:	Education
Job Title of Lead Person:	Ayesha Allen, Virtual School Head
Author / Main Contact, including their job title (if different from above):	-

In addition to this policy, local authorities and other commissioners may have their own policies, procedures and guidance which Services must comply with. These policies should complement this policy.

However, there may be additional requirements put in place by local authorities and other commissioners and these must be adhered to. Changes must not be made to Salutem's policies and procedures without corporate approval but, where needed, local procedures should be developed to accompany these.

EQUALITY AND DIVERSITY STATEMENT

The Salutem Group is committed to the fair treatment of all in line with the Equality Act 2010. An equality impact assessment has been completed on this policy to ensure that it can be implemented consistently regardless of any such factors and all will be treated with dignity and respect.

3. Headings

This policy must be brought to the attention of all employees.
The controlled version of this policy and its associated documents are available on the Blink Hub. Printed or downloaded copies are uncontrolled and may not be up to date.

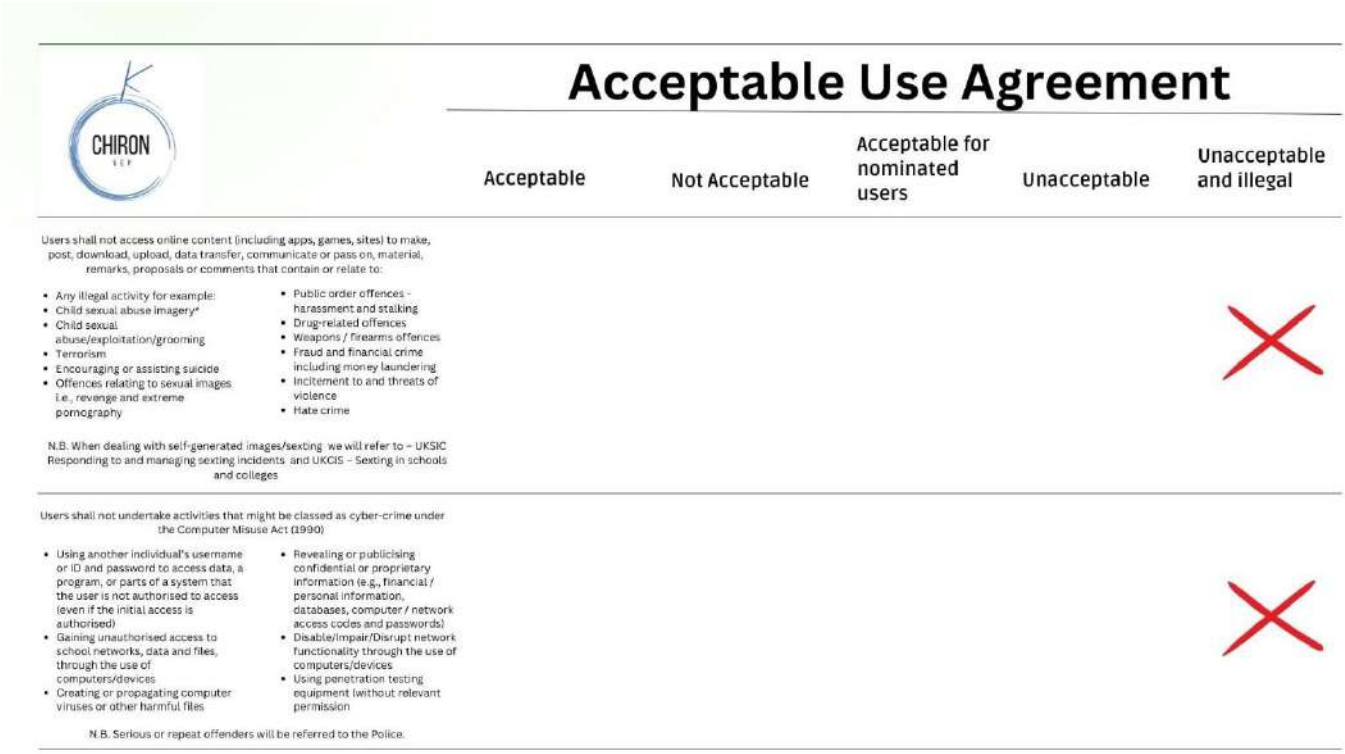
4. Content

Acceptable Use

Chiron OEP has defined what it regards as acceptable/unacceptable use and this is shown in the tables below. The Online Safety Policy and acceptable use agreements (see appendix) define acceptable use at the school. The acceptable use agreements will be communicated/re-enforced through:

- Learner induction
- staff induction and handbook
- digital signage
- communication with parents/carers
- built into education sessions
- school website

CHIRON	Acceptable Use Agreement				
		Acceptable	Not Acceptable	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not undertake activities that are not illegal but are classed as unacceptable in school	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 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	
	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	



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
- staff users should immediately report to CPOMs 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. Student should report to either a trusted member of staff or using the anonymous "I'm concerned about" button on our website.

- relevant policies and permissions should be followed when posting information online e.g., school website and social media. Only school e-mail addresses should be used to identify members of staff and learners.

Responding to incidents

The 2021 Ofsted "Review of Sexual Abuse in Schools and Colleges" highlighted the need for schools to understand that reporting systems do not always respond to the needs of learners. While the report looks specifically at harmful sexual behaviours, schools may wish to address these issues more generally in reviewing their reporting systems. The Ofsted review suggested:

- "School and college leaders should create a culture where sexual harassment and online sexual abuse are not tolerated, and where they identify issues and intervene early to better protect children and young people. ..In order to do this, they should assume that sexual harassment and online sexual abuse are happening in their setting, even when there are no specific reports, and put in place a whole-school approach to address them. This should include:
- routine record-keeping and analysis of sexual harassment and sexual violence, including online, to identify patterns and intervene early to prevent abuse"

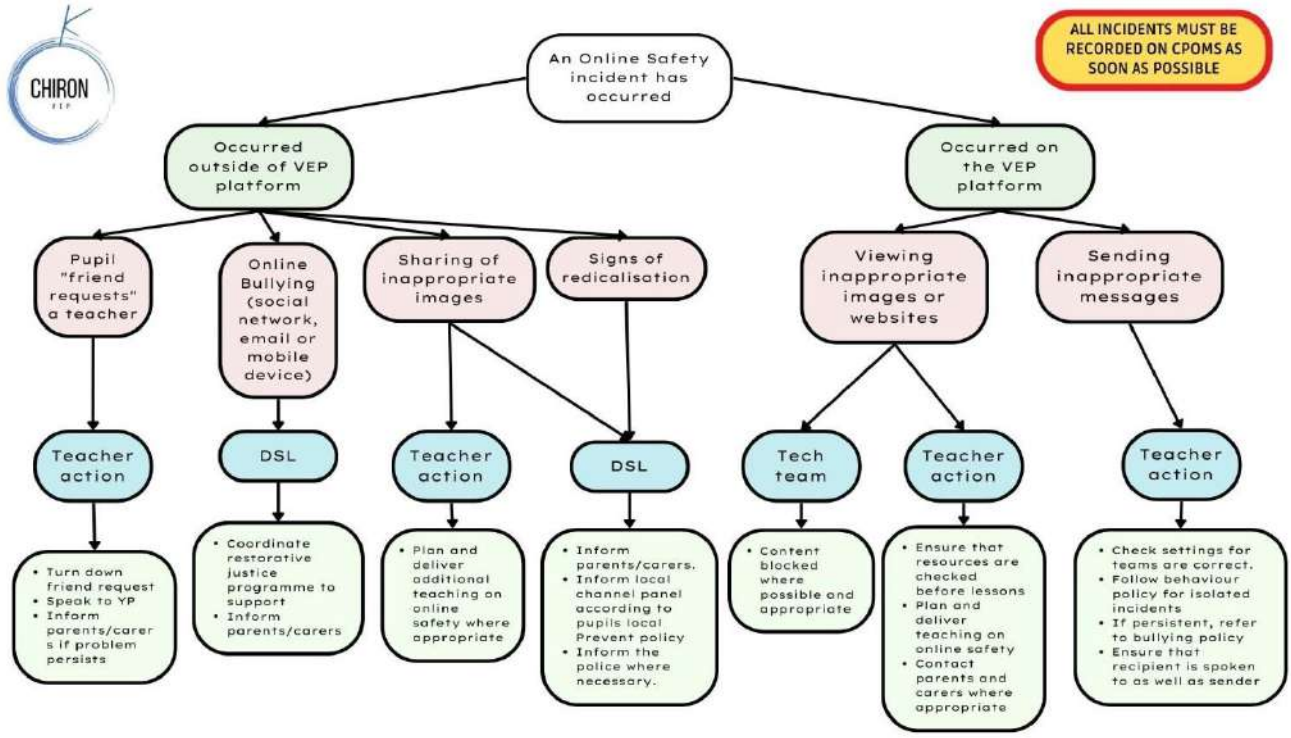
The school will take all reasonable precautions to ensure online safety for all school users but recognises that incidents may occur inside and outside of the school (with impact on the school) which will need intervention. The school will ensure:

- there are clear reporting routes which are understood and followed by all members of the school community which are consistent with the school safeguarding procedures, and with the whistleblowing, complaints and managing allegations policies.
- all members of the school community will be made aware of the need to report online safety issues/incidents
- reports will be dealt with as soon as is practically possible once they are received
- if there is any suspicion that the incident involves any illegal activity or the potential for serious harm (see flowchart below), the incident must be escalated through the agreed school safeguarding procedures.
- any concern about staff misuse will be reported to the Principal, unless the concern involves the Principal, in which case the Salutem Whistleblowing Policy should be followed (available on our website)
- 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.
    - 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:

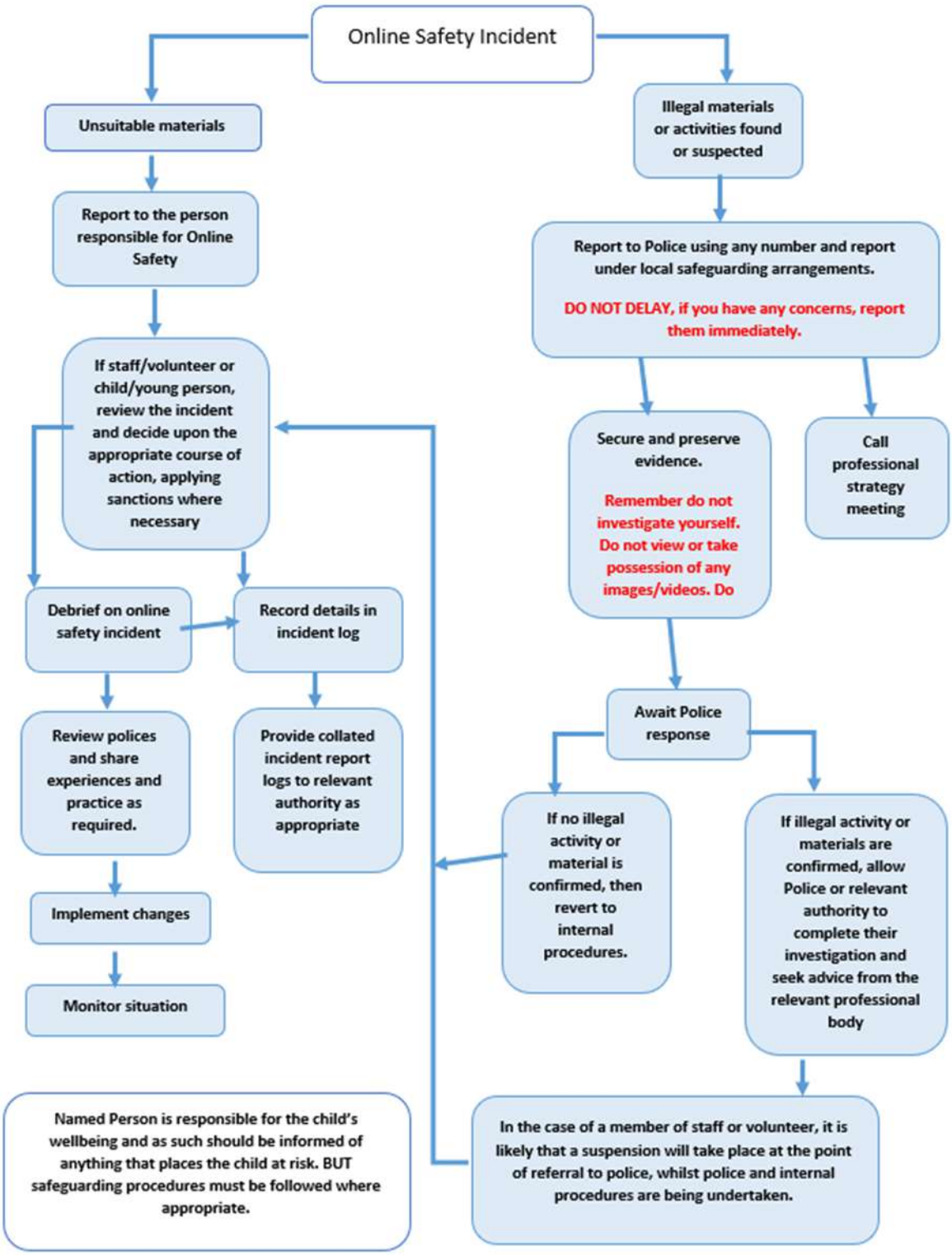
- internal response or discipline procedures
- involvement by local authority / MAT (as relevant)
- police involvement and/or action

- 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 CPOMs immediately in accordance with our safeguarding policy.
- 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
  - local authority/external agencies, as relevant (The Ofsted Review into Sexual Abuse in Schools and Colleges suggested "working closely with Local Safeguarding Partnerships in the area where the school or college is located so they are aware of the range of support available to children and young people who are victims or who perpetrate harmful sexual behaviour")
- The school will make the flowcharts below available to staff to support the decision-making process for dealing with online safety incidents.

Incident flow-chart for staff



Incident flow-chart for DSL actions



5. Areas of Governance

This policy has been written with expert contribution from appropriate stakeholders. The Information Governance team will monitor, reflect on and gain organisational learning from the implementation of this policy. This policy will be reviewed and updated two years from implementation unless legal changes demand a more timely amendment.

The application of this policy and its associated documents is mandatory for all services staff, volunteers, agency staff and all other Salutem representatives. Staff understanding of this policy and associated documents will be assured through training, assessment of competency and supervision.

Staff understanding of this policy will be assured through training and the delivery of awareness raising workshops as deemed necessary by Divisional Management. The people we support will be involved in the review to ensure it captures the important issues for them.

6. Areas of Responsibility

The Principal

- The Principal has a duty of care for ensuring the safety (including online safety) of members of the school community and fostering a culture of safeguarding.
- The Principal 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 Principal is responsible for ensuring that the Online Safety Lead, technical staff, 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 Principal 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 Ambito Quality Assurance Team:

The Quality Assurance Team will monitor the effectiveness of this policy by:

- regular meetings with the Principal
- regularly receiving (collated and anonymised) reports of online safety incidents
- checking that provision outlined in the Online Safety Policy (e.g. online safety education provision and staff training is taking place as intended)
- reporting back findings to Salutem SLT

The DSL

The Designated Safeguarding Lead should be trained in online safety issues and be aware of the potential for serious safeguarding issues to arise from:

- sharing of personal data 3
- access to illegal/inappropriate materials
- inappropriate online contact with adults/strangers
- potential or actual incidents of grooming
- online bullying.

The Online Safety Lead (DSL) will:

- take day-to-day responsibility for online safety issues, being aware of the potential for serious child protection concerns
- 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
- receive reports of online safety incidents4 and create a log of incidents to inform future online safety developments
- provide (or identify sources of) training and advice for staff/governors/parents/carers/learners

- liaise with Salutem technical staff, pastoral staff and support staff (as relevant)
- meet regularly with the online safety governing advisor to discuss current issues, review (anonymised) incidents and if possible, filtering and monitoring logs

School 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 have the relevant training to ensure that they are in control of the virtual space (e.g. turning off peer chat facilities and creating a lobby for the classroom)
- 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 the DSL (Via Nourish) for investigation/action, in line with the school safeguarding procedures
- all digital communications with learners and parents/carers should be on a professional level and only carried out using official school systems
- online safety issues are embedded in all aspects of the curriculum and other activities
- 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 spaces in accordance with the Code of Conduct
- 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
- all lessons are recorded and shared on the google classroom, only the teacher will be recorded on the video
- have 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.

The Network Manager

The network manager (via Salutem Care and Jigsaw24) 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 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 Principal 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 software/systems are implemented and regularly updated as agreed in school policies

Students

- 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

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
- publish information about appropriate use of social media relating to posts concerning the school

Parents and carers will be encouraged to support the school in:

- reinforcing the online safety messages provided to learners in school
- the use of their children's personal devices in the school (where this is allowed)

7. Learning and Development

Salutem is committed to ensuring that all staff are aware of what is expected of them so that everyone is appropriately supported. Staff should speak to their line manager in relation to their learning needs using supervision and through the appraisal process.

The school will ensure that the Designated Safeguarding Lead, Online Safety Lead and other responsible staff have appropriate skills and training to deal with online safety risks.

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 Designated Safeguarding Lead will receive regular updates through attendance at external training events, 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 DSL will provide advice/guidance/training to individuals as required.*

8. Associated Documents

Local Safeguarding Policy

Whistleblowing Policy

Data protection policy

9. Useful Links

https://swgfl.org.uk/online-safety/

10. Version Control

This is a controlled document. As a controlled document, any printed copies of this document, or saved onto local or network drives should be actively monitored to ensure the latest version is always available.

Version Number	Date	Status	Changes
V1.0	June 2023	New	New policy