LINWOOD SCHOOL
NEW! ONLINE SAFETY POLICY
Reviewed September 2025

Created by:	Nicola Cannings,
Date:	September 2025
Reviewed by:	Nicola Cannings (DSL)
Equality Impact Assessed:	
Date:	15/1/2024 01/09/2025 Updated March 2026
Next Review Date:	Autumn Term 2026

This policy applies to all members of the school community (including staff, students, 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).

Contents

Scope of online Safety Policy

This Online Safety Policy outlines the commitment of *Linwood 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, students, 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).

Linwood 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 Safeguarding Panel made up of:

- Executive Headteacher
- Senior Management and Leaders
- Designated Safeguarding and Deputy Designated Safeguarding Leads (All campuses)
- Online safety lead
- ICT Leads
- Governors

The implementation of this policy will be monitored by the DSLs. Monitoring will take place as part of the whole team meetings, which happen weekly and also throughout CPOMS © chronology reviews throughout the school year. E-safety also forms part of the reports sent to Governors termly.

Should serious online safety incidents take place, the following agencies may be informed/referred to:

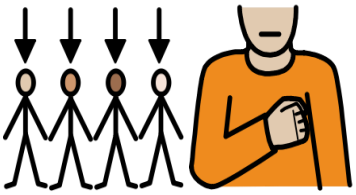
- Local Authority Safeguarding Team (e.g. BCP Multi-Agency Safeguarding Hub (MASH))
- Safer Schools Community Team & Dorset Police

The school will monitor the impact of the policy using:

- *Logs of reported incidents on CPOMS ©.*
- *Monitoring logs of internet activity (including sites visited)/filtering via Securus.*
- *Internal monitoring data for network activity.*
- *Feedback from students.*
- *Feedback from parents and carers.*

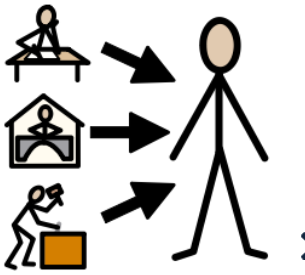
Policy and Leadership

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.

Governors



The DfE guidance "Keeping Children Safe in Education" states:
"Governing bodies and proprietors should ensure there are appropriate policies and procedures in place in order for appropriate action to be taken in a timely manner to safeguard and promote children's welfare …. this includes … online safety"

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy e.g. by asking questions about the 360Safe Audit and actions taken as well as asking for reporting on e-safety as part of Governor reports.

This review will be carried out by the Safeguarding Governor and Full Governing Board 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 Online Safety Lead from the DSL Team/SMLT.
- 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 to relevant governors group/meeting.*
- *Occasional review of the filtering change control logs and the monitoring of filtering logs (where possible).*

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

The 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 may be delegated to the Online Safety Lead/ Senior Leaders.
- The Executive Headteacher and (at least) another member of the senior leadership team on each campus 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 Executive Headteacher/Senior Leaders are responsible for ensuring that the Online Safety Lead/DSLs, 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 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 Online Safety Lead/DSLs.

Online Safety Lead/DSL

The overall online Safety Lead for Linwood School is Nicola Cannings. The DSLs at each campus are responsible for the day-to-day responding to incidents with regards to online safety and reporting and recording their actions and rationales on CPOMS ©.

The Online Safety Lead/DSL will:

- Lead the Safeguarding Panel, which includes e-safety.
- Work closely with DSLs from across all campuses on a day-to-day basis.
- 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.
- Monitor e-safety reports on CPOMS © and that the appropriate actions have been taken.
- Provide training and advice for staff, governors, parents, carers and students.
- Meet with the safeguarding governor and focus on e-safety issues within the school.
- Monitor the school's filtering system, Securus, regularly.
- Report regularly to the Executive Headteacher and Governors.

Designated Safeguarding Leads (DSLs)

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

"The designated safeguarding lead should take lead responsibility for safeguarding and child protection (**including online safety**). This should be explicit in the role holder's job description." … Training should provide designated safeguarding leads with a good understanding of their own role, … so they … 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."

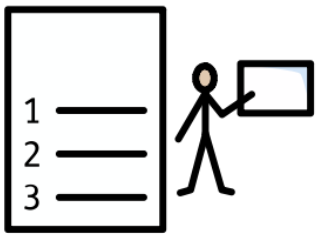
The Designated Safeguarding Leads should be trained in online safety issues and be aware of the potential for serious safeguarding issues to arise from:

- Sharing of personal data.
- Access to illegal/inappropriate materials.
- Inappropriate online contact with adults/strangers.
- Potential or actual incidents of grooming.

Curriculum Leads/Safeguarding Panel

Curriculum Leads will work with the Online Safety Lead/DSL to develop a planned and coordinated online safety education programme

This will be provided through:



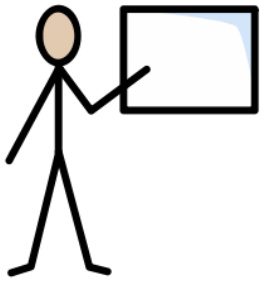
- A discrete programme.
- PHSE and RSE programmes.
- A mapped cross-curricular programme.
- Assemblies and pastoral programmes.
- Through relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week.

The Safeguarding Team also meets with the following colleagues regularly:

- Online Safety Lead.
- DSLs from all campuses.
- ICT Subject Leaders.
- PSHE Subject Leader.
- Technical Staff.

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 the campus DSL or Executive Headteacher (if related to staff breach of safeguarding practice) for investigation/action, in line with the school safeguarding procedures.
- All digital communications with students and parents/carers should be on a professional level and only carried out using official school systems including their school Outlook email address and Arbor.
- Online safety issues are embedded in all aspects of the curriculum and other activities.
- Ensure students 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, use of smart watches etc., in lessons and other school activities (where allowed) and implement current policies regarding these devices.
- In lessons where internet use is pre-planned 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 lessons take place using live-streaming or video-conferencing, staff must have full regard to national safeguarding guidance and local safeguarding policies.
- Have a zero-tolerance approach to incidents of online-bullying, sexual harassment, discrimination, hatred etc and report incidences of this immediately to the DSL and place their concern on CPOMS ©.
- 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/ Technical Teams

The network manager/technical Teams *are* 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.
- 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 DSL of the relevant campus or Executive Headteacher (where this is regarding a staff member) investigation and action.
- Monitoring software/systems are implemented and regularly updated as agreed in school policies.

Students

In line with our school's Regulation and Engagement pathways, those who are able to access the Logical pathway, those who attend CHI or Summerwood campus, and who can be an independent user of technology, they:

- Are responsible for using the school digital technology systems in accordance with the student 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 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.

- In line with our school's Regulation and Engagement pathways, those who require an assisted or advocated pathway will be supported by staff to ensure they are using the school digital technology systems in accordance with the student acceptable use agreement and Online Safety Policy.

    - Should, with support, be able to understand and report abuse, misuse or access to inappropriate materials.

- Should be supported (either by staff or parents/carers) to adopt 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.

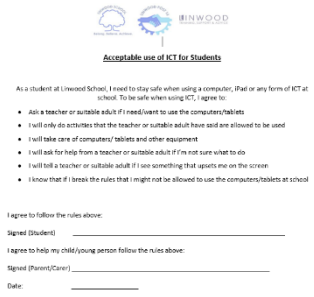
Families / Parents / Carers

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's online safety policy on the school website.
- Providing parents/carers with a copy of the Student Acceptable Use Agreement.
- Providing an opportunity for parents/carers to access The National Online College for E-safety courses and documents giving advice and guidance specifically to parents around e-safety.
- Holding events via the Family Support Team to support parents develop their understanding of E-safety.
- Seeking their permissions concerning digital images, cloud services etc.
- Placing information on the school website Safeguarding section and newsletters to bring awareness to parents of campaigns and literature.
- Supporting their children to uphold the school's policies and procedures in school in relation to personal devices, including that of smart-watches and personal mobile phones

Acceptable Use



Acceptable use of ICT for Students

As a student at Linwood School, I need to stay safe when using a computer, iPad or any form of ICT at school. To be safe when using ICT, I agree to:

- Ask a teacher or suitable adult if I need/want to use the computers/tablets
- I will only do activities that the teacher or suitable adult have said are allowed to be used
- I will take care of computers/ tablets and other equipment
- I will ask for help from a teacher or suitable adult if I'm not sure what to do
- 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 that I might not be allowed to use the computers/tablets at school

I agree to follow the rules above:

Signed (Student) _____

I agree to help my child/young person follow the rules above:

Signed (Parent/Carer) _____

Date: _____

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. At Linwood School they are signed or acknowledged by their staff as part of their conditions of employment. It is also required that students and parents/carers sign them, though it is more important for these to be understood and followed rather than just signed.

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 N.B. Schools should refer to guidance about dealing with self-generated images/sexting – UKSIC Responding to and managing sexting incidents and UKCIS – Sexting in schools and colleges					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					X

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
	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). Serious or repeat offences will be reported to the police. Under the Cyber-Prevent agenda the National Crime Agency has a remit to prevent students becoming involved in cyber-crime and harness their activity in positive ways					
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). This is only acceptable by nominated users when researching for the purposes of education e.g. PSHE lessons regarding the topics mentioned.			X	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	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 should be given for the following activities when undertaken for non-educational purposes: PDO (Personal Device Only)	Staff and other adults				Students			
	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	X				X			
Online Shopping			X	X	X			X CHI and Summerwood
Social Media			X	X	X			X CHI and Summerwood
Entertainment Streaming e.g. Netflix & Disney+ used within the purposes of learning, where content is appropriate and/or approved by a member of SMLT			X		X			X CHI and Summerwood
Mobile phones being bought in to school **Please note that the school takes no responsibility for the loss or damage of personal devices.**			X				X	
Use of mobile phones at social times			X		X			X CHI and Summerwood
Taking photos on personal mobile phones	X				X			X CHI and Summerwood
Use of smart watches when messaging, photo features and calls are switched to Do Not Disturb, off or Flight Mode so that the watch feature can be used but no access to social media or messaging. **Please note that watches that can take photos without the use of a phone or secondary device are not allowed. This applies to everyone.**		X				X		X CHI and Summerwood
	Not allowed	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission/ awareness
Use of other personal devices e.g. tablets, gaming devices Students: only when needed for Regulation and Engagement as set out in PREP, agreed by a member of SMLT and under supervision. The school takes no responsibility for loss or damage of personal devices.			X				X	X CHI and Summerwood

Use of other personal devices e.g. tablets, gaming devices Students: only when needed for Regulation and Engagement as set out in PREP, agreed by a member of SMLT and under supervision. The school takes no responsibility for loss or damage of personal devices.			X				X	X CHI and Summerwood

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 students 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 the DSL or Executive Headteacher, 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.

Reporting and Responding to concerns raised

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. Staff can report via CPOMS © their concerns about students and the website enables reporting via our form online or confidentially via email to the school Business Manager.
- All members of the school community will be made aware of the need to report online safety issues/incidents within the regulation and engagement pathways accessible to each individual.
- 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 the incident must be escalated through the agreed school safeguarding procedures.

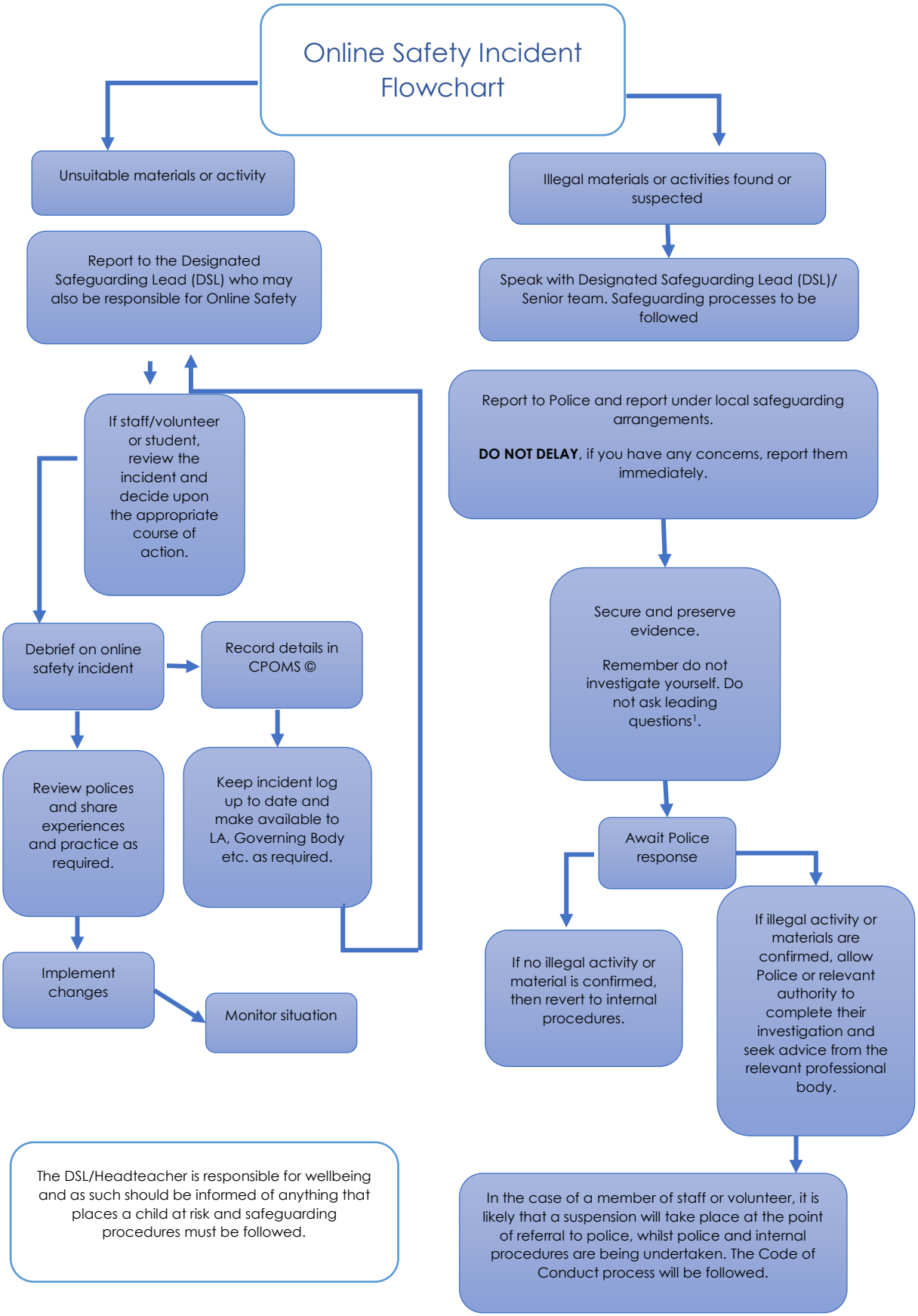
- Any concern about staff misuse will be reported to the Executive Headteacher, unless the concern involves the Executive Headteacher, in which case the complaint is referred to the Chair of Governors and the Local Authority Designated Officer (LADO).
- Where there is no suspected illegal activity, devices 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 students 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 stored on CPOMS© or StaffSafe©.
  - 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.

- There are support strategies in place e.g., access to the Employee Assistance Programme.
- Incidents should be logged on CPOMS © for students and Confide © for staff.
- 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 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.
  - Students, through assemblies/lessons.
  - Parents/carers, through newsletters, school social media, website.
  - Governors, through regular safeguarding updates.
  - Local authority/external agencies, as relevant.

Online Safety Incident Flowchart



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 regulation and engagement procedures as follows:

Responding to Student Actions

Responding to student actions will include the appropriate action in accordance with the student's regulation and engagement pathway, taking into consideration individual barriers to learning. All of our approaches will be personalised as much as possible. Actions may include some of the following, depending on the severity of the incident:

- Informing parents/carers/guardians.
- Involving the class teacher in education both personalised and curriculum based.
- Removal of network access or internet access.
- Repair and Reflect meetings (in conjunction with regulation and engagement pathways).
- Referral to the Executive Headteacher / DSL / Phase Leader.
- Internal exclusion or suspension.
- Referral to Dorset Police / Social Care / MASH and other outside agencies including Safer Schools Community Team.

Incidents that can result in some or all of the above actions being taken include:

- Deliberately accessing or trying to access material that could be considered illegal.
- Attempting to access or accessing the school network, using another user's account (staff or student) or allowing others to access school network by sharing username and passwords.
- Sending an e-mail, text or message that is regarded as offensive, harassment or of a bullying nature.
- Using proxy sites or other means to subvert the school's filtering system.
- Unauthorised use of online services.
- Accidentally accessing offensive or pornographic material and failing to report the incident.
- Unauthorised use of digital devices (including taking images).
- Continued infringements of the above, following previous warnings or consequences.

Education (Students)

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 Phases and year groups against the nationally agreed framework, taking into consideration the barriers our students face and removing those barriers to the best of our ability.
- An inclusive approach to lessons to meet the needs of all students, including context-relevant learning.
- Digital competency is planned and effectively threaded through the appropriate digital pillars in other curriculum areas e.g. PHSE; SRE; Literacy etc.
- Students should 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.
- Where students are allowed to freely search the internet, staff should be vigilant in supervising the students 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.

Staff & Volunteers (Training)

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.
- 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 Safeguarding training and the school's 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 (will receive regular updates through attendance at external training events, (e.g. UKSIC / SWGfL / 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 Online Safety Lead (or other nominated person) will provide advice/guidance/training to individuals as required.

Governors (Training)

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 or other relevant organisation (e.g., SWGfL).
- Participation in school training / information sessions for staff or parents (this may include attendance at assemblies/lessons).

A higher level of training will be made available to (at least) the Online Safety Governor.

Families

Many parents and carers have only 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 online 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 seek to provide information and awareness to parents and carers through:

- Providing parents with the opportunity to access The National College/ National Online Safety Website to have their own account. This enables parents to access video tutorials and leaflets (https://nationalcollege.com/parents).
- Providing opportunities to engage with the Family Support Team through workshops specifically targeting online safety.
- Sharing information with parents/Carers via our social media pages, MIS, newsletters and events.
- Reference to the relevant web sites/publications, e.g. SWGfL; www.saferinternet.org.uk/; www.childnet.com/parents-and-carers.

Technical Infrastructure/equipment, Monitoring and Filtering.

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.

- 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 who have the cognitive capacity at KS2 and above will be provided with a username and secure password by (ICT technical team) who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password. Linwood School use group or class logons and passwords for KS1 and working at that level or below.
    - The "administrator" passwords for the school systems, used by the Network Manager (or other person) must also be available to the Headteacher or other nominated senior leader and kept in a secure place (e.g. school safe).
    - The Network Manager 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 or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes.
    - Internet filtering/monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet.
    - 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

agreement. Linwood School uses SWGfL filtering system and Securis to monitor activity.

- An appropriate system is in place via CPOMS ©. for staff and to teachers for students 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, work stations, 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 devices are protected by up to date virus software.
- An agreed policy is in place regarding the extent of personal use that users (staff/students/community users) and their family members are allowed on school devices that may be used out of school.
- An agreed policy is in place that forbids staff from downloading executable files and installing programmes on school devices.

Mobile Technologies

Mobile technology devices may be school owned/provided or personally owned and might include smartphone, tablet, wearable devices, notebook/laptop or other technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider internet which may include the school learning platform and other cloud-based services such as e-mail and data storage.

All users should understand that the primary purpose of the use of mobile/personal devices in a school context is educational. The mobile technologies policy should be consistent with and inter-related to other relevant school polices including but not limited to those for safeguarding, behaviour, anti-bullying, acceptable use, and policies around theft or malicious damage. Teaching about the safe and appropriate use of mobile technologies should be an integral part of the school's online safety education programme.

In preparing a mobile technologies policy the school should consider possible issues and risks. These may include:

- Security risks in allowing connections to your school network.
- Filtering of personal devices.
- Breakages and insurance.
- Access to devices for all students.
- Avoiding potential classroom distraction.
- Network connection speeds, types of devices.
- Charging facilities.
- Total cost of ownership.

A range of mobile technology strategies is possible. However, these need to be thoroughly researched, risk assessed and aligned with existing policy prior to implementation.

The school acceptable use agreements for staff, students, 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 device	Student owned	Staff owned	Visitor owned
Allowed in school	Yes	Yes	Yes	Yes	Yes	Yes
Full network access	Yes	Yes	Yes	No	No	No
Internet only						
No network access				Yes	Yes	Yes

Social media

With widespread use of social media for professional and personal purposes a policy that sets out clear guidance for staff to manage risk and behaviour online is essential. Core messages should include the protection of students, the school and the individual when publishing any material online.

Expectations for teachers' professional conduct are set out in the DfE Teachers Standards but all adults working with children and young people must understand that the nature and responsibilities of their work place them in a position of trust and that their conduct should reflect this.

All schools and local authorities have a duty of care to provide a safe learning environment for students and staff. Schools could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, bully online, discriminate on the grounds of sex, race, or disability or who defame a third party may render the school liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

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

- Ensuring that personal information is not published.
- Education/training being provided including 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 students, parents/carers.

School staff should ensure that:

- No reference should be made in social media to students, 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.
- The school permits reasonable and appropriate access to personal social media sites during school hours when the member of staff is on their breaks and in an area of the school where students are not e.g. the staff room.

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 development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and students need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for online bullying 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. It is common for employers to carry out internet searches for information about potential and existing employees.

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. Guidance can be found on the SWGfL Safer Remote Learning web pages and in the DfE Safeguarding and remote education.
- When using digital images, staff will inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images.
- Staff/volunteers must be aware of those students 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). 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 *students* in the digital/video images. Events where this applies will be made clear to parents/carers.
- Staff and volunteers are allowed to take digital/video images to support educational aims (for example, Evidence for learning), 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 students are appropriately dressed.
- 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 Online Safety Policy.
- Students' full names will not be used anywhere on a website or blog, particularly in association with photographs.

- Written permission from parents or carers will be obtained before photographs of students are taken for use in school or published on the school website/social. 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.
- Students' work can only be published with the permission of the student and parents/carers.

Online Publishing

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

- Public-facing website
- Social media
- Online newsletters
- Email
- Text messages

The school website is managed/hosted by The Collective. The school ensures that the 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 student work, images or videos are published, their identities are protected, and full names are not published.

The school public online publishing provides information about online safety e.g., publishing the schools Online Safety Policy and acceptable use agreements; curating latest advice and guidance; news articles etc, adding online safety advice to the safeguarding section of the website.

The website includes an online reporting process for parents and the wider community to register issues and concerns to complement the internal reporting process.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the current data protection legislation.

- Please see the school's Data Protection and Privacy Policy for full details.

Links with other documents and policies

- Data protection policy
- Safeguarding and Child Protection Policy
- Staff and Volunteer Acceptable Use of ICT Policy Agreement
- Linwood School Pupil ICT Agreement