Online Safety Policy

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

**This policy was adopted by the Governing Body in November 2024.
It is reviewed annually.**

This policy is due for review November 2025

Scope of the Online Safety Policy

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

This Online Safety Policy applies to all members of the school community (including staff, learners, 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).

Liscard Primary 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 *[SLT/ Online Safety Committee and the members of the Governor Teaching and Learning Committee]* made up of:

- *Headteacher/senior leaders*
- *online safety lead*
- *staff – including teachers/support staff/technical staff*
- *governors*
- *parents and carers*
- *learners (where appropriate)*

Schedule for development, monitoring and review

This Online Safety Policy was approved by the *school governing body on:*	*TBC Autumn 2*
The implementation of this Online Safety Policy will be monitored by:	*Sue Talbot and SLT*
Monitoring will take place at regular intervals:	*Each Term*
The *governing body* **will receive a report on the implementation of the Online Safety Policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals:**	*Governors Meeting –* *Headteacher's Report to Governors*
The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new technological developments, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	*July 25*
Should serious online safety incidents take place, the following external persons/agencies should be informed:	*LADO Police CEOP*

Process for monitoring the impact of the Online Safety Policy

The school will monitor the impact of the policy using:

- *logs of reported incidents*
- *monitoring logs of internet activity (including sites visited)*
- *internal monitoring data for network activity*
- *surveys/questionnaires of:*
  - *learners*
  - *parents and carers*
  - *staff.*

Policy and leadership

Responsibilities

To ensure the online safeguarding of members of our school community it is important that all members of that community work together to develop safe and responsible online behaviours, learning from each other and from good practice elsewhere, reporting inappropriate online behaviours, concerns, and misuse as soon as these become apparent. While this will be a team effort, the following sections outline the online safety roles and responsibilities of individuals and groups within the school.

Headteacher and senior leaders

- The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community and fostering a culture of safeguarding, though the day-to-day responsibility, where necessary, may be delegated to the Online Safety Lead.
- The Headteacher and other members of the senior leadership team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.
- The Headteacher/senior leaders are responsible for ensuring that the 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 Headteacher/senior leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role.
- The Headteacher/senior leaders will receive regular monitoring reports from the Online Safety Lead.

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.

The teaching and learning committee, whose members will receive regular information about online safety incidents and monitoring reports, will carry out this review. A member of the governing body will take on the role of Online Safety Governor to include:

- **meetings with the Online Safety Lead**
- **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*** *teaching and learning committee*
- membership of the school Online Safety Group
- 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.

Online Safety Lead/s
The Online Safety Lead will:
- lead the Online Safety Group
- work closely on a day-to-day basis with the Designated Safeguarding Lead (DSL), where these roles are not combined
- alongside the headteacher, 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 incidents 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 (school/local authority/external provider) technical staff, pastoral staff and support staff (as relevant)
- meet with the online safety governor to discuss current issues, review (anonymised) incidents and if possible, filtering and monitoring logs
- attend relevant governing body meetings/groups
- report regularly to the Headteacher/senior leadership team.
- liaises with the local authority or relevant body where appropriate.

Designated Safeguarding Lead (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
- access to illegal/inappropriate materials
- inappropriate online contact with adults/strangers
- potential or actual incidents of grooming
- online bullying inclusive of potential misuse of generative AI in relation to 'deep fakes'

Curriculum Team
The appropriate Curriculum Teams will work with the Online Safety Lead to develop a planned and coordinated online safety education programme supported by **Project EVOLVE** .

This will be provided through a combination of:
- a discrete programme
- PHSE and SRE programmes
- A mapped cross-curricular programme
- assemblies and pastoral programmes
- through relevant national initiatives and opportunities e.g. Safer Internet Day and **Anti-bullying week**. etc.

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 a member of SLT for I 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 technologies, mobile devices, cameras, etc., in lessons and other school activities (where allowed) and implement current policies regarding these devices
- in lessons where internet use is pre-planned learners 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 and should take note of the guidance contained in the the remote teaching and learning policy
- have a zero-tolerance approach to incidents of online-bullying inclusive of misuse of generative AI, sexual harassment, discrimination, hatred etc
- 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 staff
The network manager/technical staff from **Hi-Impact** 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/DfE 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 a member of SLT 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

Learners
- are responsible for using the school digital technology systems in accordance with the learner acceptable use agreement and Online Safety Policy
- should understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- should know what to do if they or someone they know feels vulnerable when using online technology
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that **the school's Online Safety Policy covers their actions out of school, if related to their membership of the school.**

Parents and carers
Parents and carers play a crucial role in ensuring that their children understand the need to use the online services and devices in an appropriate way.

The school will take every opportunity to help parents and carers understand these issues through:
- publishing the school Online Safety Policy on the school website
- providing them with a copy of the learners' acceptable use agreement
- publish information about appropriate use of social media relating to posts concerning the school
- seeking their permissions concerning digital images, cloud services etc **(see parent/carer AUA in the appendix)**

- parents'/carers' evenings, newsletters, website, social media and information about national/local online safety campaigns and literature.

Parents and carers will be encouraged to support the school in:
- reinforcing the online safety messages provided to learners in school
- the use of their children's personal devices in the school (where this is allowed)

Community users

Community users who access school systems/website/learning platforms as part of the wider school provision will be expected to sign a community user AUA before being provided with access to school systems. **(A community user's acceptable use agreement template can be found in the appendices).**

Online Safety Committee

The Online Safety Committee provides a consultative group that has representation from the school community, with responsibility for issues regarding online safety and monitoring the Online Safety Policy including the impact of initiatives:

The Online Safety Group has the following members:
- Online Safety Lead
- Designated Safeguarding Lead
- senior leaders
- online safety governor
- technical staff
- teacher and support staff members
- learners
- parents/carers

Members of the Online Safety Committee will assist the Online Safety Lead with:
- the production/review/monitoring of the school Online Safety Policy/documents
- the production/review/monitoring of the school filtering policy and requests for filtering changes if needed
- mapping and reviewing the online safety education provision – ensuring relevance, breadth and progression and coverage
- reviewing network/filtering/monitoring/incident logs, where possible
- encouraging the contribution of learners to staff awareness, emerging trends and the school online safety provision
- consulting stakeholders – including staff/parents/carers about the online safety provision
- monitoring improvement actions identified through use of the 360-degree safe self-review tool.

Professional Standards

There is an expectation that required professional standards will be applied to online safety as in other aspects of school life i.e., policies and protocols are in place for the use of online communication technology between the staff and other members of the school and wider community, using officially sanctioned school mechanisms.

Online Safety Policy

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

"Online safety and the school or college's approach to it should be reflected in the child protection policy" Latest policy can be found on the school website or via request at the school office.

The school Online Safety Policy:
- sets expectations for the safe and responsible use of digital technologies for learning, administration, and communication
- allocates responsibilities for the delivery of the policy
- is regularly reviewed in a collaborative manner, taking account of online safety incidents and changes/trends in technology and related behaviours
- establishes guidance for staff in how they should use digital technologies responsibly, protecting themselves and the school and how they should use this understanding to help safeguard learners in the digital world
- describes how the school will help prepare learners to be safe and responsible users of online technologies
- establishes clear procedures to identify, report, respond to and record the misuse of digital technologies and online safety incidents, including external support mechanisms
- is supplemented by a series of related acceptable use agreements
- is made available to staff at induction and through normal communication channels including CPD and Google Spaces
- **is published on the school website.**

Acceptable use

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

Acceptable use agreements

The Online Safety Policy and acceptable use agreements define acceptable use at the school. The acceptable use agreements will be communicated/re-enforced through:
- staff induction and handbook
- posters/notices around where technology is used
- communication with parents/carers
- built into education sessions
- school website
- peer support.

Acceptable Use

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 See - **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 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) N.B. The School will decide whether these should be dealt with internally or by the police. Serious or repeat offences will be reported to the police. Under the Cyber-Prevent agenda the National Crime Agency has a remit to prevent learners becoming involved in cyber-crime and harness their activity in positive ways – further information here					X
Users shall not undertake activities that are not illegal but are classed as unacceptable in school policies:	Accessing inappropriate material/activities online in a school setting including pornography, gambling, drugs. (Informed by the school's filtering practices and/or AUAs)			X	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	

	Acceptable Use					
User actions		**Acceptable**	**Acceptable at certain times**	**Acceptable for nominated users**	**Unacceptable**	**Unacceptable and illegal**
	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**	

	Staff and other adults				Learners			
Consideration should be given for the following activities when undertaken for <u>non-educational</u> purposes:	**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/commerce			**X** on own devices		**X**			
File sharing			**X** on own devices		**X**			
Social media			**X** on own devices		**X**			
Messaging/chat			**X** on own devices		**X**			
Entertainment streaming e.g. Netflix, Disney+	**X**				**X**			
Use of video broadcasting, e.g. YouTube, Twitch, TikTok	**X**				**X**			
Mobile phones may be brought to school		**X**						**X**
Use of mobile phones for learning at school	**X**				**X**			
Use of mobile phones in social time at school		**X**			**X**			
Taking photos on mobile phones/cameras	**X**							**X**
Use of other personal devices, e.g. tablets, gaming devices	**X**							**X**
Use of personal e-mail in school, or on school network/wi-fi			**X** on own devices		**X**			
Use of school e-mail for personal e-mails	**X**				**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 email addresses, text messaging or social media must not be used for these communications.*
- **staff should be expected to follow good practice when using personal social media regarding their own professional reputation and that of the school and its community**
- **users should immediately report to a nominated person – in accordance with the school policy – the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication**
- *relevant policies and permissions should be followed when posting information online e.g., school website and social media. Only school email addresses should be used to identify members of staff and learners.*
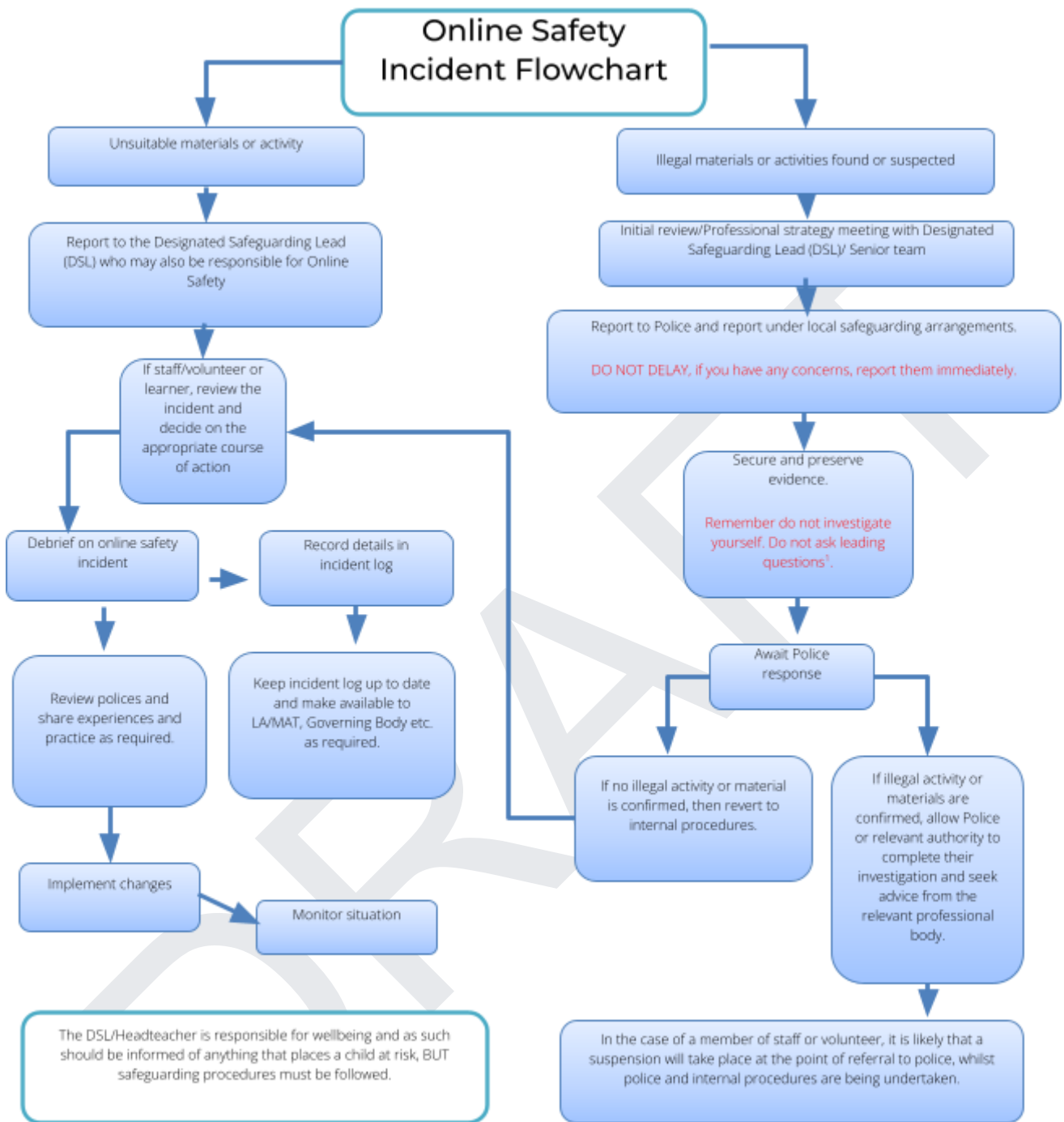
Reporting and responding

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

- **There are clear reporting routes which are understood and followed by all members of the school community which are consistent with the school safeguarding procedures, and with the whistleblowing, complaints and managing allegations policies.**
- **All members of the school community will be made aware of the need to report online safety issues/incidents**
- **reports will be dealt with as soon as is practically possible once they are received**
- **The Designated Safeguarding Lead, Online Safety Lead and other responsible staff have appropriate skills and training to deal with online safety risks.**
- **If there is any suspicion that the incident involves any illegal activity or the potential for serious harm (see flowchart and user actions chart in the appendix), the incident must be escalated through the agreed school safeguarding procedures.**
- Any concern about staff misuse will be reported to the Headteacher, unless the concern involves the Headteacher, in which case the complaint is referred to the Chair of Governors and the local authority.
- Where there is no suspected illegal activity, devices may be checked using the following procedures:
    - one or more senior members of staff should be involved in this process. This is vital to protect individuals if accusations are subsequently reported.
    - conduct the procedure using a designated device that will not be used by learners and, if necessary, can be taken off site by the police should the need arise (should illegal activity be subsequently suspected). Use the same device for the duration of the procedure.
    - ensure that the relevant staff have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
    - record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed, and attached to the form
    - once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
        - o internal response or discipline procedures
        - o involvement by local authority (as relevant)
        - o 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 - Master File and blank templates can be found in the Headteacher's office.
- 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 (as relevant)
    - learning from the incident (or pattern of incidents) will be provided) 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 school will make the flowchart below available to staff to support the decision-making process for dealing with online safety incidents.

Online Safety Incident Flowchart

Online Safety Incident Flowchart

Unsuitable materials or activity

Report to the Designated Safeguarding Lead (DSL) who may also be responsible for Online Safety

If staff/volunteer or learner, review the incident and decide on the appropriate course of action

Debrief on online safety incident

Record details in incident log

Review polices and share experiences and practice as required.

Keep incident log up to date and make available to LA/MAT, Governing Body etc. as required.

Implement changes

Monitor situation

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

Illegal materials or activities found or suspected

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

Report to Police and report under local safeguarding arrangements.

DO NOT DELAY, if you have any concerns, report them immediately.

Secure and preserve evidence.

Remember do not investigate yourself. Do not ask leading questions[1].

Await Police response

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

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

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

School actions

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

Responding to Learner Actions

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

Responding to Staff Actions

Incidents	Refer to line manager	Refer to Headteacher/ Principal	Refer to local authority /HR	Refer to Police	Refer to LA / Technical Support Staff for action re filtering, etc.	Issue a warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities)		X	X	X				
Deliberate actions to breach data protection or network security rules.		X	X	X	X	X		X
Deliberately accessing or trying to access offensive or pornographic material		X	X	X	X	X	X	X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		X			X			X
Using proxy sites or other means to subvert the school's filtering system.		X			X	X		X
Unauthorised downloading or uploading of files or file sharing		X			X	X		X
Breaching copyright or licensing regulations.		X	X		X	X		X
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account.		X				X		
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		X	X			X		X
Using personal email/social networking/messaging to carry out digital communications with learners and parents/carers		X	X	X **Where necessary**	X	X	X	X
Inappropriate personal use of the digital technologies e.g. social media / personal email		X				X		X
Careless use of personal data, e.g. displaying, holding or transferring data in an insecure manner		X				X		X
Actions which could compromise the staff member's professional standing		X	X			X		X
Actions which could bring the school into disrepute or breach the integrity or the ethos of the school.		X	X			X		X
Failing to report incidents whether caused by deliberate or accidental actions		X	X			X		X
Continued infringements of the above, following previous warnings or sanctions.		X	X			X		X

Online Safety Education Programme

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 is broad, relevant and provides progression, with opportunities for creative activities and will be provided in the following ways

- A **planned online safety curriculum** for all year groups matched against a nationally agreed framework e.g. **Education for a Connected Work Framework by UKCIS/DCMS** and **regularly taught in a variety of contexts.**
- **Lessons are matched to need; are age-related and build on prior learning**
- **Lessons are context-relevant with agreed objectives leading to clear and evidenced outcomes**
- **Learner need and progress are addressed through effective planning and assessment**
- **Digital competency is planned and effectively threaded through the appropriate digital pillars in other curriculum areas e.g. PHSE; SRE; Literacy etc**
- **it incorporates/makes use of relevant national initiatives and opportunities e.g.** Safer Internet Day **and** Anti-bullying week
- **the programme will be accessible to learners at different ages and abilities such as those with additional learning needs or those with English as an additional language.**
- *learners should be helped to understand the need for the learner 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 learners should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches*
- *where learners are allowed to freely search the internet, **staff should be vigilant in supervising** the learners and monitoring the content of the websites the young people visit **especially during unstructured times***
- **the online safety education programme should be relevant and up to date to ensure the quality of learning and outcomes.**

Contribution of Learners

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

- mechanisms to canvass learner feedback and opinion.
- appointment of digital leaders/anti-bullying ambassadors/peer mentors etc
- the Online Safety Group has learner representation where appropriate
- learners contribute to the online safety education programme e.g. peer education, digital leaders leading lessons for younger learners, online safety campaigns
- learners designing/updating acceptable use agreements
- contributing to online safety events with the wider school community e.g. parents' evenings, family learning programmes etc.

Staff/volunteers

All staff will receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- a planned programme of formal online safety and data protection training will be made available to all staff. This will be regularly updated and reinforced.
- the training will be an integral part of the school's annual safeguarding and data protection training for all staff
- all new staff will receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and acceptable use agreements. It includes explicit reference to classroom management, professional conduct, online reputation and the need to model positive online behaviours

- the Online Safety Lead and Designated Safeguarding Lead (or other nominated person) will receive regular updates through attendance at external training events, (e.g. UKSIC / LA / other relevant organisations) and by reviewing guidance documents released by relevant organisations
- this Online Safety Policy and its updates will be presented to and discussed by staff in staff/team meetings/INSET days
- the Designated Safeguarding Lead/Online Safety Lead (or other nominated person) will provide advice/guidance/training to individuals as required.

Governors

Governors should take part in online safety training/awareness sessions, with particular importance for those who are members of any sub-committee/group involved in technology/online safety/health and safety/safeguarding. This may be offered in several ways such as:
- attendance at training provided by the local authority or other relevant organisation
- 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

The school will seek to provide information and awareness to parents and carers through:
- regular communication, awareness-raising and engagement on online safety issues, curriculum activities and reporting routes
- regular opportunities for engagement with parents/carers on online safety issues through awareness communication / parent/carer evenings etc
- the learners – who are encouraged to pass on to parents the online safety messages they have learned in lessons and by learners leading sessions at parent/carer evenings.
- letters, newsletters, website, etc
- high profile events / campaigns e.g. Safer Internet Day
- reference to the relevant websites/publications, e.g. SWGfL; www.saferinternet.org.uk/; www.childnet.com/parents-and-carers (see Appendix for further links/resources).
- Sharing good practice with other schools in clusters and or the local authority

Adults and Agencies

The school will provide opportunities for local community groups and members of the wider community to gain from the school's online safety knowledge and experience. This may be offered through the following:
- online safety messages targeted towards families and relatives.
- *providing family learning courses in use of digital technologies and online safety where appropriate/when needed*
- *the school will provide online safety information via their website and social media for the wider community*
- *supporting community groups, e.g. early years settings, childminders, youth/sports/voluntary groups to enhance their online safety provision*

Technology

Working closely with our Technical Support provider Hi-Impact the school ensures that the provider carries out all the online safety and security measures. Hi-Impact are fully aware of the school Online Safety Policy/acceptable use agreements and the school has a Data Processing Agreement in place with them. DPAs are also completed with the take on of any new systems especially cloud based.

The school is responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. The school should ensure that all staff are made aware of policies and procedures in place on a regular basis and explain that everyone is responsible for online safety and data protection.

Filtering

- the school filtering policies are agreed by senior leaders and technical staff and are regularly reviewed and updated in response to changes in technology and patterns of online safety incidents/behaviours
- the school manages access to content across its systems for all users. The filtering provided meets the standards defined in the UK Safer Internet Centre Appropriate filtering.
- access to online content and services is managed for all users
- illegal content (e.g., child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list and the police assessed list of unlawful terrorist content, produced on behalf of the Home Office. Content lists are regularly updated
- there are established and effective routes for users to report inappropriate content
- there is a clear process in place to deal with requests for filtering changes (see Appendix for more details).
- *the school has (if possible) provided enhanced/differentiated user-level filtering (allowing different filtering levels for different abilities/ages/stages and different groups of users: staff/learners, etc.)*
- *younger learners will use child friendly/age-appropriate search engines e.g. Swiggle*
- filtering logs are regularly reviewed and alert the school to breaches of the filtering policy, which are then acted upon.
- *where personal mobile devices have internet access through the school network, content is managed in ways that are consistent with school policy and practice.*
- *access to content through non-browser services (e.g. apps and other mobile technologies) is managed in ways that are consistent with school policy and practice.*

Monitoring

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

- **The school monitors all network use across all its devices and services.**
- **An appropriate monitoring strategy for all users has been agreed and users are aware that the network is monitored. There is a staff lead responsible for managing the monitoring strategy and processes.**
- **There are effective protocols in place to report abuse/misuse. There is a clear process for prioritising response to alerts that require rapid safeguarding intervention. Management of serious safeguarding alerts is consistent with safeguarding policy and practice**
- **Technical monitoring systems are up to date and managed and logs/alerts are regularly reviewed and acted upon.**

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

- physical monitoring (adult supervision in the classroom)
- internet use is logged, regularly monitored and reviewed
- filtering logs are regularly analysed and breaches are reported to senior leaders
- *pro-active alerts inform the school of breaches to the filtering policy, allowing effective intervention.*
- *where possible, SLT and school technical staff regularly monitor and record the activity of users on the school technical systems*

Technical Security

The 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 are securely located and physical access restricted
- there are rigorous and verified back-up routines, including the keeping of network-separated (air-gapped) copies off-site or in the cloud. We have a rolling backup drive that is replaced each Friday, a physical backup to the backup server and a cloud backup that does FMS and the network shared areas. Saas protection is also in place to backup the Google Shared drives.
- **all users have clearly defined access rights to school technical systems and devices. Details of the access rights available to groups of users will be recorded by the Network Manager (or other person) and will be reviewed, at least annually**
- **all users (adults and learners) have responsibility for the security of their username and password and must not allow other users to access the systems using their log on details. Users must immediately report any suspicion or evidence that there has been a breach of security**
- **all school networks and systems will be protected by secure passwords. Passwords must not be shared with anyone. All users will be provided with a username and password** by Admin or Tech support (Hi-Impact) who will keep an up-to-date record of users and their usernames **the master account passwords for the school systems are kept in a secure place,**
- **passwords should be long and including capital letters, numbers and other characters other then letters etc**
- records of learner usernames and passwords for learners in Key Stage 1 or younger can be kept in an electronic or paper-based form, but they must be securely kept when not required by the user. *Password complexity for younger learners may be reduced (for example 6 character maximum) and should not include special characters. Where external systems have different password requirements the use of random words or sentences should be encouraged*
- password requirements for learners at Key Stage 2 and above should increase as learners progress through school
- The Business manager supported by Tech Support is responsible for ensuring that all software purchased by and used by the school is adequately licensed and that the latest software updates (patches) are applied.
- 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 and devices 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 endpoint (panda antivirus) software. This is managed by Hi-Impact
- an agreed policy is in place for the provision of temporary access of 'guests', (e.g., trainee teachers, supply teachers, visitors) onto the school systems
- an agreed policy is in place regarding the extent of personal use that users (staff / learners / 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 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. The use of removable media is discouraged with cloud storage being the main source of storage.
- systems are in place that prevent the unauthorised sharing of personal data unless safely encrypted or otherwise secured. (See school personal data policy)

Artificial intelligence (AI)

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard.

Liscard Primary School recognises that AI has many uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.

Liscard Primary School will treat any use of AI to bully pupils in line with our anti bullying policy.

Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used by the school.

Mobile technologies

The school acceptable use agreements for staff, learners, parents, and carers outline the expectations around the use of mobile technologies.

The school allows:

	School devices			Personal devices		
	School owned for individual use	School owned for multiple users	Authorised 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	**N/A**	**N/A**	**N/A**	**No**	**Yes** where Appropriate	**Yes**
No network access	**N/A**	**N/A**	**N/A**	**Yes**	**N/A**	**Yes**

Staff and learners who have been allocated a School owned device should know:

- *to whom they will be allocated*
- *where, when and how their use is allowed – times/places/in/out of school*
- *if personal use is allowed*
- *levels of access to networks/internet (as above)*
- *management of devices/installation of apps/changing of settings/monitoring*
- *network/broadband capacity*
- *technical support*
- *filtering of devices*
- *access to cloud services*
- *use on trips/events away from school*
- *data protection*
- *taking/storage/use of images*
- *exit processes, what happens to devices/software/apps/stored data if user leaves the school*
- *liability for damage*
- *staff training.*

Personal devices - Staff and learners need to know:-

- *which users are allowed to use personal mobile devices in school (staff/learners/visitors)*
- *restrictions on where, when and how they may be used in school*
- *if used in support of learning, how staff will plan their lessons around the potential variety of device models and different operating systems*
- *storage*
- *whether staff will be allowed to use personal devices for school business*
- *levels of access to networks/internet*
- *network/broadband capacity*
- *technical support*
- *filtering of the internet connection to these devices and monitoring the access*
- *management of software licences for personally owned devices.*
- *data protection*
- *taking/storage/use of images*
- *liability for loss/damage or malfunction following access to the network (likely to be a disclaimer about school responsibility)*
- *identification/labelling of personal devices*
- *how visitors will be informed about school requirements*
- *how education about the safe and responsible use of mobile devices is included in the school online safety education programmes*
- *how misuse will be dealt with*

Social media

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to learners through:
- ensuring that personal information is not published
- education/training being provided 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 learners, parents/carers

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

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

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

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.

Digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and learners instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and learners 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 DfE Safeguarding and remote education
- **when using digital images, staff will inform and educate learners about the risks associated with the taking, use, sharing, publication and distribution of images.**
- **staff/volunteers must be aware of those learners whose images must not be taken/published. Those images should only be taken on school devices. The personal devices of staff should not be used for such purposes**
- In accordance with **guidance from the Information Commissioner's Office**, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is 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 *learners* in the digital/video images
- staff and volunteers are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, storage, distribution and publication of those images
- care should be taken when sharing digital/video images that learners are appropriately dressed
- learners must not take, use, share, publish or distribute images of others without their permission
- photographs published on the website, or elsewhere that include learners will be selected carefully and will comply with Online Safety Policy
- **learners' full names will not be used anywhere on a website or blog, particularly in association with photographs**
- **permission from parents or carers will be obtained before photographs of learners are taken for use in school or published on the school website/social media.** (see parents and carers acceptable use agreement in the Appendix). 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**
- learners' work can only be published without names

Online Publishing
The school communicates with parents/carers and the wider community and promotes the school through :
- Public-facing website - School Spider
- Class Dojo
- Social media - Twitter
- Online newsletters
- email etc

The school website is managed/hosted by **School Spider**. The school ensures that online safety policy has been followed in the use of online publishing e.g., use of digital and video images, copyright, identification of young people, publication of school calendars and personal information – ensuring that there is least risk to members of the school community, through such publications.

Where learners work, images or videos are published, their identities are protected, and full names are not published.

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, creating an online safety page on the school website.

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

The school:
- **has a Data Protection Policy.** **See data protection policy for more details**
- **implements the data protection principles and can demonstrate that it does so**
- **has paid the appropriate fee to the Information Commissioner's Office (ICO)**

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

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

Staff must ensure that they:
- at all times take care to ensure the safekeeping of personal data, minimising the risk of its loss or misuse
- can recognise a possible breach, understand the need for urgency and know who to report it to within the school
- can help data subjects understand their rights and know how to handle a request whether verbal or written and know who to pass it to in the school
- only use encrypted data storage for personal data
- will not transfer any school personal data to personal devices. Procedures are in place to enable staff to work from home (i.e. VPN access to the school network, or a work laptop provided).
- use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data
- transfer data using encryption, a secure email account (where appropriate), and secure password protected devices.

Outcomes

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

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

Policy Evaluation				
Points to be considered	Yes	No	N/A	Please supply evidence
● Policy annually reviewed	✔			Shared with all stakeholders, approved by governors and published on the school website
● Policy in line with current legislation	✔			Annual review to ensure any statutory changes or updates in policies are included.
● Coordinator in place	✔			Yes – SLT
● Nominated governor in place	✔			
● Coordinator carries out role effectively	✔			As identified through performance management and feedback from the headteacher
● Headteacher, coordinator and nominated governor work closely	✔			Regular meetings and updates to governors via sub committee
● Policy endorsed by governing body	✔			
● Policy regularly discussed at meetings of the governing body	✔			See governor meeting minutes
● School personnel aware of this policy	✔			
● School personnel comply with this policy	✔			
● Pupils aware of this policy	✔			Online Safety Agreements and Rules in Place and shared with Pupils
● Parents aware of this policy	✔			Published on the website
● Visitors aware of this policy	✔			SLT share relevant aspects with visitors
● Local community aware of this policy	✔			Published on the website
● Funding in place	✔			
● Policy complies with the Equality Act	✔			
● Equality Impact Assessment undertaken	✔			
● Policy referred to in the School Handbook		✔		
● Policy available from the school office		✔		On website but a paper copy can be printed on request
● Policy available from the school website	✔			
● School Council involved with policy development		✔		
● All stakeholders take part in questionnaires and surveys		✔		
● All associated training in place	✔			
● All outlined procedures complied with	✔			
● Linked policies in place and up to date	✔			
● Associated policies in place and up to date	✔			

A statement outlining the overall effectiveness of this policy	

The policy ensures that all the school community are aware of the statutory duties around Online Safety and what is expected of all staff, pupils and parents to ensure that these duties are met. The policy clearly sets out how the school will support children through clear Online Safety procedures and curriculum planning.

Policy Approval Form

Policy Title:	Online Safety Policy					Date when written:		November 24	
Policy written by:	Jane Fagan				New Policy (✓ or x)		Revised Policy (✓ or x)		✔
Stakeholders consulted in policy production: (✓ or x)	Governors	Senior Leadership Team	Teaching Personnel	Support Personnel	Administrative Personnel	Parents	Pupils		Local Community
	✔	✔	✔	✔	✔	✔	✔		
Date when approved by Governors:	November 24	Date when presented to stakeholders:	November 24		Date when implemented:	November 24			
Published on: (✓ or x)	School Website		School Prospectus			Staff Handbook			
	✔								