'Loving to Learn, Learning to Love'

Online Safety Policy

Last Approved: September 2023

Review Date: September 2024

Online Safety Policy

Contents

Development/Monitoring/Review of this Policy

This online safety policy has been developed by a working group made up of

- Headteacher
- Online Safety Officer/Coordinator
- Staff – including teachers, support staff, technical staff
- Local Governing Board
- Parents and carers

Consultation with the whole school community will take place through a range of formal and informal meetings.

Development/Monitoring/Review of the Internet Safety

This online safety policy was approved by the Local Governing Board on:	November 2023
The implementation of this online safety policy will be monitored by the:	Headteacher, Designated Safeguarding Leader and Designated Safeguarding Link Governor
Monitoring will take place at regular intervals:	Termly
The Local Governing Board 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:	Termly – Headteacher reports at Full Governing Board meetings
The online safety policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	September 2024
Should serious online safety incidents take place, the following external persons/agencies should be informed:	Stoke-on-Trent Safeguarding Children Partnership, the Orchard Community Trust, LADO, Police

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of suspicious internet activity through Securus filtering software
- Internal monitoring data for network activity and Internet use
- Surveys/questionnaires of
    - pupils
    - parents/carers
    - staff

Scope of the Policy

This policy applies to all members of St Mark's CE Primary School, including staff, pupils, volunteers, parents/carers, visitors and community users that have access to and are users of school digital technology systems, both in and out of the school.

The **Education and Inspections Act 2006** empowers Headteachers to regulate the behaviour of pupils when they are off the school site, and also empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This includes and is pertinent to incidents of online-bullying or other online safety incidents covered by this policy, regardless of if these incidents take place outside when related to the membership of the school.

The **2011 Education Act** increased these powers with regard to the searching for, and of, electronic devices, in the suspect of the deletion of data. In the case of both acts, action can only be taken over issues covered by the school's published Behaviour Management Policy.

The school will address any such incidents within this policy, and associated behaviour and anti-bullying policies, and will inform parents/carers of incidents of inappropriate online safety behaviour that take place either in or out of school.

Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within the school.

Local Governing Board

The Local Governing Board are responsible for the approval of this online safety policy and for reviewing its effectiveness when in practice.

The Governors will carry out reviews through the receipt of regular information about online safety incidents and monitoring reports. A member of the Local Governing Board has taken on the role of Online Safety Governor and the role of the Online Safety Governor includes:

- regular meetings with the Online Safety Leader
- attendance at Online Safety Group meetings
- regular monitoring of online safety incident logs
- regular monitoring of filtering/change control logs
- reporting to relevant Governors/Board/Committee/meeting

Headteacher and Senior Leaders

The Headteacher, Deputy Headteacher and Designated Safeguarding Leader have a duty of care for ensuring the safety (including online safety) of all members of the school community.

- Headteacher, Deputy Headteacher and Designated Safeguarding Leader know the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.
    - (See flow chart on dealing with online safety incidents – Appendix 1 - "Responding to incidents of misuse" and relevant Local Authority/Orchard Community Trust/other relevant body disciplinary procedures).

    - Online Safety BOOST (https://boost.swgfl.org.uk/) is an 'Incident Response Tool' that outlines the steps (and forms to complete) any staff facing an issue, disclosure or report, need to follow.
- Headteacher, Deputy Headteacher and Designated Safeguarding Leader are responsible for ensuring that all staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- Headteacher, Deputy Headteacher and Designated Safeguarding Leader 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 Senior Leadership Team will receive regular monitoring reports from the Online Safety Lead.

Online Safety Lead

At St. Mark's CE Primary School, the Safeguarding Leader Miss J Thomas is the appointed Online Safety Leader, and has the responsibility to:

- lead the Online Safety Group
- any occurring online safety issues and has a leading role in establishing and reviewing the school online safety policies or documents
- ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- provide training and advice for staff
- liaise with the Local Authority/Orchard Community Trust and other relevant bodies where appropriate
- liaise with school technical staff
- receive reports of online safety incidents and creates a log of incidents to inform future online safety developments,
    - Online Safety BOOST includes access to Whisper, an anonymous reporting app that installs onto a school website and extends the schools ability to capture reports from staff, children and parents https://boost.swgfl.org.uk/
- meet regularly with the Online Safety Governor to discuss current issues, review incident logs and filtering/change control logs

Network Manager/Technical staff:

RM I.T. Support (Mr. W. Weaver), together with the over watch of the Online Safety Leader are responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets required online safety technical requirements and any Local Authority/Orchard Community Trust online safety policies that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy.
- the filtering policy and online tracking service (Securus) is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person

    - all staff have the responsibility to report and ensure, through regular monitoring, that this is maintained, proactive and in line with current trends to promote the overall welfare of all stakeholders, including all staff, children and parents/carers.
- that 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.
- that the use of the networks/internet/digital technologies is regularly monitored in order that any misuse/attempted misuse can be reported to the Safeguarding Lead and Senior Leaders;
- that monitoring and record systems are implemented, maintained and updated as agreed in school policies

Teaching and Support Staff

Are responsible for ensuring that:

- they have an up-to-date awareness of online safety matters and of the current school online safety policy and practices
- they have read, understood and signed the staff acceptable use agreement.
- they report any suspected misuse or problem to the Safeguarding Lead (Online Safety Lead) and Senior Leadership for investigation/action.
- all digital communications with pupils/parents/carers should be on a professional level and only carried out using official school systems .
- online safety issues, and safer Internet practice are embedded in all aspects of the curriculum and extra-curricular activities.
- pupils understand and follow the Online Safety Policy and acceptable use policies
    - all children are to sign the appropriate acceptable use policy, and these records are kept with the class teacher
- they monitor the use of digital technologies, mobile devices, cameras, etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices in lessons, where internet use is pre-planned, pupils should be guided to sites checked as suitable for their use and that processes and reporting procedures are in place for dealing with any unsuitable material that is found in internet searches.

Designated Safeguarding Lead

Is trained in recognising online safety issues and is fully aware of the potential for serious child protection/safeguarding issues which may arise from:

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

In support of this role, the Designated Safeguarding Lead is a pivotal member of the Online Safety Group, sharing full access to any reports created, which may indicate the potential for any child to come to harm through Internet use, both in, and out of school.

- Where any harm may be suspected, teachers must report concerns on the appropriate Safeguarding forms, in line with the School Child Protection Policy.

Online Safety Group

The Online Safety Group provides a review group that has wide representation from the school community, with responsibility for issues regarding online safety and the monitoring the Online Safety Policy including the impact of initiatives. The group will also be responsible for regular reporting to the Governing Body/Directors.

Members of the Online Safety Group 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, together with a review of the online tracking service: Securus.
- mapping and reviewing the online safety/digital literacy curricular provision – ensuring relevance, breadth and progression.
- monitoring network/internet/filtering/incident logs.
- consulting stakeholders – including parents/carers and the pupils about the online safety provision.
- monitoring improvement actions identified through use of the 360 degree safe self-review tool.

It must be understood that all stakeholders, including pupils and parents, have the right to be educated and safeguarded in all risks of Internet use, both in school and out. It must therefore also be recognised that these stakeholders take the responsibilities outlined below, together in agreement with a signed acceptable use policy.

Pupils:

- are responsible for using the school digital technology systems in accordance with the pupil acceptable use agreement.
- to develop a good understanding of research, recognising inappropriate or unwanted online material.
- need to understand the importance of reporting abuse, misuse or any access to inappropriate materials and know how to do so.
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking/use of images and on online-bullying.
- 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 it is related to their membership of the school.

Parents/carers

Parents/carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website, and information about national/local online safety campaigns.

Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events.

- access to parents' sections of the website/Learning Platforms (including Purple Mash) and on-line pupil records (where this has been published).
- their children's personal devices in the school (where this has been permitted).

Policy Statements

Education – Pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety and Safer Internet practices is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

The education of Safer Internet practice should be embedded across all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum is too designed in a way that is broad and relevant, providing progression, with opportunities for creative activities. This will be provided in the following ways:

- A planned online safety curriculum that is built as part of the wider curriculum and is regularly reviewed to develop good practice.
    - Planning for the online safety curriculum at St. Mark's CE has been written in line with the SWGfL Project Evolve, providing a clear and progressive learning journey to promote online safety and personal wellbeing throughout the school.
    - This supports Foundation Stage learning through to Year 6, and beyond.
- Key online safety messages should be reinforced as part of a planned programme of assemblies.
- Pupils should be taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information.
- Pupils should be taught to acknowledge the source of information used, recognising the copyright ownership of materials accessed on the internet
- Pupils should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.
    - This is supported by and integrated within the school PSHE curriculum, to promote the understanding of community, identity and keeping each other safe.
    - The Counter Terrorism and Securities Act 2015 requires schools to ensure that children are safe from terrorist and extremist material on the internet.
- Pupils should be helped to understand the need for the pupil acceptable use agreement and encouraged to adopt safe and responsible use both within and outside school.
    - 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, pupils 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 pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.

    - Any incidents of inappropriate content being viewed must be reported to the Network Manager and Online Safety Lead to investigate to ensure the content is after that filtered.
    - Any such incidents must then be shared with Parents to promote communication and a line of enquiry to prevent escalation.
- It is accepted that from time to time, for good educational reasons, pupils may need to research topics (e.g. racism, drugs, and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff or the Designated Online Safety Lead to temporarily remove those sites from the filtered list for the period of study.
    - Any request to do so, should be auditable, with clear reasons for the need.

Education – Parents/carers

Although many parents and carers may only have a limited understanding of online safety risks and issues, they play an essential role in the education of their children and in the monitoring 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 therefore seek to provide information and awareness to parents and carers through:

- Letters, newsletters,
- Information on the school web site or Online Learning Platforms
    - Including reference to the relevant web sites/publications e.g. swgfl.org.uk, www.saferinternet.org.uk/, http://www.childnet.com/parents-and-carers and CEOP (the Child Exploitation and Online Protection Command).
    - Implementation of the CEOP command is integrated within the School Website
- High profile events or campaigns e.g., Safer Internet Day or Online Safety Webinars

Education & Training – Staff/Volunteers

It is essential that all staff receive online safety training and understand their responsibilities, as outlined previously in this policy.

Training will be offered as follows:

- A planned programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced. Including the use of Online Safety BOOST online webinars (https://boost.swgfl.org.uk/)
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and acceptable use agreements.
- This online safety policy and its updates will be presented to and discussed by staff in staff/team meetings/training sessions.

Technical – infrastructure/equipment, filtering and monitoring

It is an important role of the school to ensure that all online safety measures are managed effectively and known issues are acted upon reliably and effectively to maximise the wellbeing of all its users.

The school has the responsibility to ensure that the all-network infrastructure is as safe and secure as is reasonably possible, and that policies and procedures approved within this policy are implemented. The school will also ensure that all staff are effective in carrying out their online safety responsibilities and implementing reporting procedures.

- School technical systems are managed in ways that ensure that the school meets recommended technical requirements and these are regularly reviewed alongside audits of the safety and security of school technical systems
- All users will have clearly defined access rights to school technical systems and devices.
- The Computing Lead and Network Technician, who will keep an up-to-date record of users and their usernames, will provide all users (including those of Foundation Stage) with a username and secure password.
    - Users are responsible for the security of their username and password.
- The "administrator" passwords for the school system, used by the Network Manager, are made available to the Headteacher, Online Safety Lead and School Business manager, enabling active use of monitoring systems and network logging.
- The School Business Manager, (Mrs. L. Bloore) and the IT Engineer (Mr William Weaver) – are 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.
    - All Illegal content (including images of an abusive nature) are filtered by the school systems by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored.
    - Any attempts to access inappropriate or illegal content (including extremist content) is monitored and tracked by SECURUS, and there is a clear process in place to deal with requests for filtering changes.
- School technical staff regularly monitor and record the activity of users on school systems and users are made aware of this in the acceptable use agreement.
- An appropriate system is in place (to be described) for users to report any actual/potential technical incident/security breach to the relevant person, as agreed).
    - An example of this is included in the Appendix.
- 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 and encryption software.
- An agreed policy is in place regarding the use of removable media (e.g., memory sticks/CDs/DVDs) by users on school devices. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured, (for further information on this, please refer to the School's GDPR policy).

Mobile Technologies

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

All users of the school internet and network systems should understand that the primary purpose of the use such devices is educational. The school mobile technologies policy is consistent with the safeguarding policy, behaviour policy, anti-bullying policy, acceptable use policy, and policies around theft or malicious damage. Teaching about the safe and appropriate use of mobile technologies is therefore and integral part of the school's online safety education programme.

- The school acceptable use agreements for staff, pupils and parents/carers give consideration to the use of mobile technologies,

- St. Mark's CE Primary School allows:

	School Devices		Personal Devices		
	School owned for single user	School owned for multiple users	Student owned	Staff owned	Visitor owned
Allowed in school	Yes	Yes	No[1]	Yes	Yes
Full network access	Yes	Yes	No	No	No
Internet only	Guest Users	Guest Users	No	No	Yes[2]

[1] Permission will be considered on a case-by-case basis for mobile devices belonging to Y6 pupils to be left in the school office where appropriate and/or necessary. This consideration is to be led by the Headteacher and Designated Safeguarding Lead.

[2] Work laptops/tablets only under the discretion of the Headteacher/SLT for example Social Workers, Health Visitors and Police.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and pupils must be aware and educated in 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:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own personal images on the internet e.g., on social networking sites.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website/social media/local press.
    - All permissions obtained by the school must be in line with the school GDPR policy.
- In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their own children for their own personal use (as such use in not covered by the Data Protection Act).
    - The school will actively promote the standing that these images must remain private and not published online, or made publicly available on social networking sites.
    - Photographs of other children on a parent's personal device, in line with the school's GDPR policy, is prohibited at all school events and any such photos must be deleted upon request.
    - It is the responsibility of all staff to be vigilant and protect the wellbeing of all children at the school.
- The taking of digital imagery to support the educational outcomes for pupils is encouraged, but must follow school policy for GDPR and abide by the digital imagery permissions obtained by parents concerning the sharing, distribution and publication of those images on any online platform.
    - All academic imagery must be taken on school equipment, where the use of personally owned equipment is prohibited and must not be used.
- Care should be taken when taking digital/video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into question or disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
    - As mentioned, this is in line with the school GDPR policy and obtained parental permission for academic photography.
- Pupils' full names will not be used anywhere on the school website, particularly in association with photographs.

Data Protection

With effect from 25th May 2018, the data protection arrangements for the UK changed following the European Union General Data Protection Regulation (GDPR). As a result, schools are subject to greater scrutiny in their care and use of personal data. Subject to the school's GDPR policy, personal data will be recorded, processed, transferred and made available in accordance to the Data Protection Act (2018) legislation.

As a result, the school will ensure that:

- the Data Protection Policy is reviewed and updated regularly, and risk assessments are conducted to maximise security

- it implements the data protection principles outlined in the school Data Protection Policy and is able to demonstrate that it does so through use of policies, notices and records, with references to digital imagery and personal information - including that of a pupil's work.
- it has clear and understood arrangements for the security, storage and transfer of personal data.
- IT system security is ensured and regularly checked. Patches and other security essential updates are applied promptly to protect the personal data on the systems. Administrative systems are secure and systems accessible in the classroom or by learners is prevented.

Staff must ensure that they:

- at all times take care to ensure the safe keeping 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
- 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

When personal data is stored on any mobile device the:

- data must be encrypted and password protected.
- device must be password protected.
- device must be protected by up-to-date virus and malware checking software
- data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete.

Pupils must ensure that they:

- do not share their log in details
- only log in as themselves
- take appropriate images/videos of other children
- do not distribute image/videos of other children

For further information, please refer to the School's Data Protection Policy, available on the school website.

Social Media - Protecting Professional Identity

All schools, academies, MATs and local authorities have a duty of care to provide a safe learning environment for all stakeholders. Schools, MATs and local authorities are held responsible, indirectly for acts of their employees in the course of their employment. Staff members that harass, engage in online bullying, discriminate on the grounds of sex, race or disability make the school or local authority/Orchard Community Trust liable to the targeted party.

The school provides the following measures to ensure reasonable steps are in place to minimise the risk of harm to pupils, staff and the school through:

- Ensuring that personal information is not published
- Ensuring that training is provided including: acceptable use; social media risks; checking of settings; data protection; reporting issues.
    - Including Online Safety BOOST online webinars (https://boost.swgfl.org.uk/)
- Clear reporting guidance, including responsibilities, procedures and sanctions – refer to 'Responding of Incidents of Misuse)

- Risk assessment, including legal risk
    - Completed by the School Business Manager and Designate Online Safety Lead

School staff must ensure that:

- No reference should be made in social media to pupils, 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 or local authority/Orchard Community Trust
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information

Personal Use:

Personal communications are those made via a personal social media account. In all cases, where a personal account is used that associates itself with the school 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.

- Personal communications that 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 private social media sites, where direct mention or discussion of school activity is actively avoided.
- All staff are advised to be mindful of their professional conduct when using internet based social networking sites.
    - If comments are published by individuals that could be deemed as detrimental to the school, this could be considered as misconduct and disciplinary action may be taken, in line with the school disciplinary procedures.
- All staff are encouraged to keep their personal social media accounts private and are also encouraged not to link with the parents of pupils on their personal social media accounts.
- Regularly updating the privacy protocols on such platforms to maintain a professional relationship with the school community.
- Under school confidentiality procedures and in accordance with GDPR, staff are prohibited from publishing any content containing work materials, identifying staff or pupils on their social media accounts.

Dealing with unsuitable/inappropriate activities

Some internet usage, including the viewing of images or videos of an abusive, sexual or racist nature, is illegal and is strictly be banned from all school technical systems. Other activities, including. Cyber-bullying is prohibited and any incidents must be reported in line with this policy and this could lead to criminal prosecution.

There are however a range of activities which may, generally, be legal but would be inappropriate in a school context. The school believes that the activities referred to in the following section are inappropriate in a school context and that all users must not engage in these activities in/or outside the school when using school owned equipment or systems.

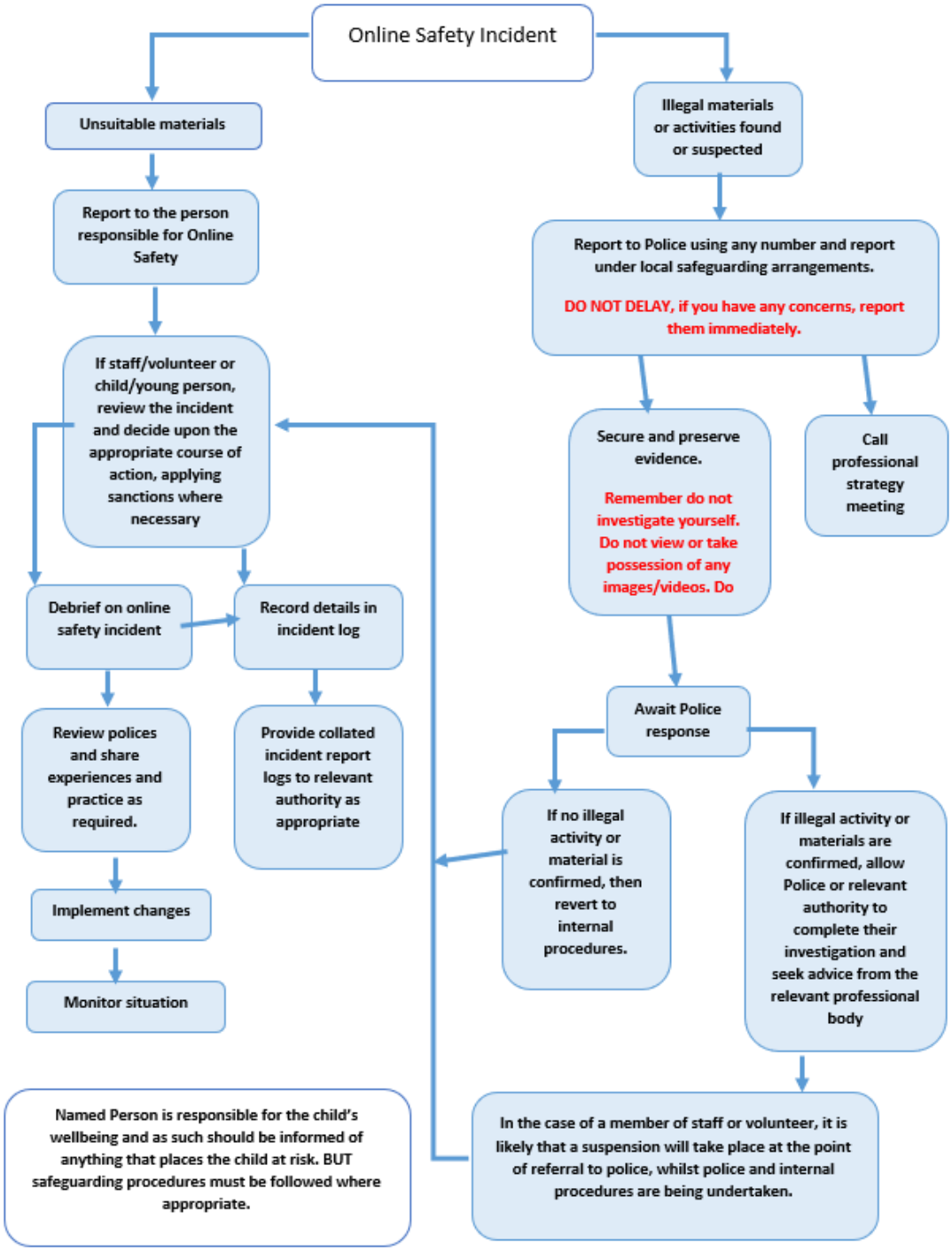
This school policy restricts usage as follows:

User Actions		Acceptable	Acceptable at certain times	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978 N.B. Schools/academies 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
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.				X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008				X
	Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986				X
	Pornography			X	
	Promotion of any kind of discrimination			X	
	threatening behaviour, including promotion of physical violence or mental harm			X	
	Promotion of extremism or terrorism			X	
	Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute			X	

Activities that might be classed as cyber-crime under the Computer Misuse Act: • 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)				X
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school			X	
Revealing or publicising confidential or proprietary information (e.g. financial/personal information, databases, computer/network access codes and passwords)			X	
Unfair usage (downloading/uploading large files that hinders others in their use of the internet)			X	
Using school systems to run a private business			X	
Infringing copyright			X	
On-line gambling			X	
On-line shopping for educational purposes	X			
Personal File sharing		X		
Use of personal social media			X	
Use of messaging apps			X	
Use of video broadcasting e.g., YouTube			X	

Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities, where this is the case all staff must refer to the following protocol:



All complaints and concerns about a pupil's internet use are to be directed to and investigated by the Online Safety Lead and class teacher. Where appropriate and necessary, this information is to also be passed onto the Designated Safeguarding Lead in line with the Anti-bullying Policy and Child Protection Policy.

Any complaint about staff misuse must be referred directly to the Headteacher. Complaints of a child protection nature must be dealt with in accordance with the school's Child Protection Policy,

Complaints and Disciplinary Policies and Procedures of the school and bought to the attention of the Headteacher.

The school adheres to the Orchard Community Trust Complaints Policy, which is available on the school website.

Signed: ……...

Headteacher

Signed: ……

Co-Chair of the Local Governing Board

Date: December 2022

Review date: September 2023

Appendices

Acceptable Use Agreement

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe access to these digital technologies.

This acceptable use agreement is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and will have good access to digital technologies to enhance their learning and will, in return, expect the pupils to agree to be responsible users.

Acceptable Use Agreement - Staff

New technologies have become integral to the lives of children and young people in today's society, both within schools/academies and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe access to the internet and digital technologies at all times.

This acceptable use policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of technology in their everyday work.

The school will try to ensure that staff and volunteers will have good access to digital technology to enhance their work, to enhance learning opportunities for pupils learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

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

For my professional and personal safety:

- I understand that the school will monitor my use of the school digital technology and communications systems.

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

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

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

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

- When I use my mobile devices in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up-to-date anti-virus software and are free from viruses.
- I will not use personal email addresses on the school ICT systems.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will ensure that my data is regularly backed up, in accordance with relevant school policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, terrorist or extremist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer.
- I will not knowingly disable or cause any damage to school equipment, or the equipment belonging to others.

- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School/LA Personal Data Policy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based documents containing personal data must be held in lockable storage.
- I understand that data protection policy requires that any staff or student/pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software however this may have happened.

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

- I understand that this acceptable use policy applies not only to my work and use of school digital technology equipment in school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school
- I understand that if I fail to comply with this acceptable use agreement, I could be subject to disciplinary action.
    - This could include a warning, a suspension, referral to Governors/directors and/or the Local Authority and in the event of illegal activities the involvement of the police.

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

Name: .....

Signed: .....

Date: .....

Acceptable Use Agreement – UKS2

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users.

For my own personal safety:

- I understand that the *school* will monitor the devices I use in school
- I will keep my username and password safe and secure; I will not share it.
- I will be aware of "stranger danger", when I am communicating on-line.
- I will not share personal information about myself or others when on-line.
- I will not meet people I have met on-line.
- I will tell a teacher about any material or messages that makes me feel uncomfortable.
- I will not impersonate anyone on-line.

I understand that everyone has equal rights to use technology as a resource and:

- I understand that the school devices are for learning, and will not use them for gaming/play unless I have permission.
- I will tell a teacher about any damage or problems with equipment or software, however this may have happened.

I will respect others online, and:

- I will only take or send images as part of my learning.
- I recognise and respect that people do not want me taking pictures of them without their permission.

When using the Internet:

- I will take care to check that the information that I access is safe, as I understand that the work of others may be fake and mislead me.

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

- I understand that there will be consequences if I misuse technology in school or at home.
- This will be in line with the School Behaviour Policy and Anti-bullying Policy.

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

- I use the school devices
- I use my own equipment out of school

Name of Pupil: .....

Class: .....

Signed: .....

Date: .....

Pupil Acceptable Use Agreement – Lower Key Stage 2

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users.

For my own personal safety:

- I understand that the *school* will look at my use of the systems, devices and digital communications.
- I will keep my username and password safe and secure.
- I will be aware of "stranger danger", when I am communicating on-line.
- I will not share personal information about myself or others when on-line
    - this could include names, addresses, email addresses, telephone numbers or age
- I will tell a teacher or trusted adult if I see anything that makes me feel uncomfortable on-line.

When using the internet for research or play, I know that:

- I will should check that the information that I access from the internet is safe and accurate, as I understand that some may be fake.

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

- I understand that there will be consequences if I misuse technology (examples would be online-bullying, use of images or personal information).
- This will be in line with the School Behaviour Policy and Anti-bullying Policy.

Name of Pupil: .....

Class: .....

Signed: .....

Date: .....

Pupil Acceptable Use – Foundation Stage and Key Stage 1

This is how we stay safe when we use computers:

I will ask a grown up if I want to use the computers/tablets

I will be good when using the computer/tablet

I will look after computers/tablets and other equipment

I will ask for help from a grown up if I am not sure what to do or if I think I have done something wrong

I will tell a grown up if I see something that upsets me on the screen

I know that if I break the rules, I might not be allowed to use a computer/tablet

Pupil Acceptable Use – Foundation Stage and Key Stage 1

This is how we stay safe when we use computers:

I will ask a grown up if I want to use the computers/tablets.

I will be good when using the computer/tablet.

I will look after computers/tablets and other equipment.

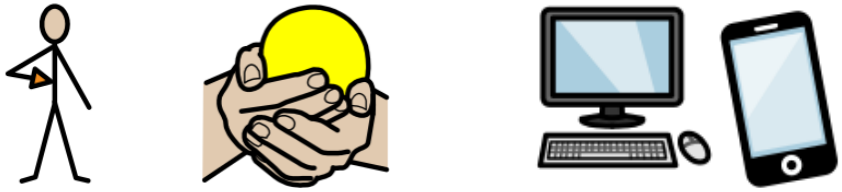
I will ask for help from a grown up if I am not sure what to do or if I think I have done something wrong.

I will tell a grown up if I see something that upsets me on the screen.

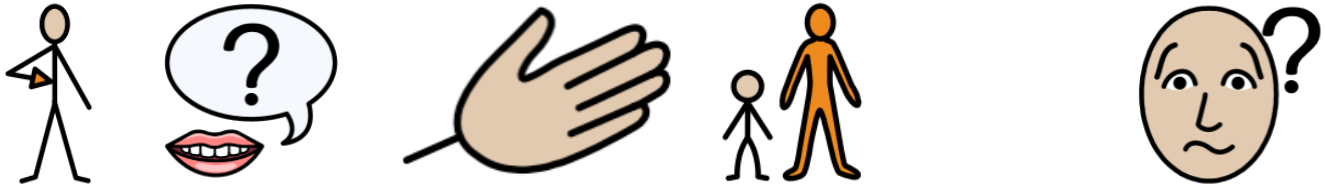
I know that if I break the rules, I might not be allowed to use a computer/tablet.

I will ask a grown up if I want to use the computers/tablets.

I will be good when using the computer/tablet.



I will look after computers/tablets and other equipment.



I will ask for help from a grown up if I am not sure what to do or if I think I have do

I will tell a grown up if I see something that upsets me on the screen.

Record of reviewing devices/internet sites (responding to incidents of misuse)

Name of child: _____

Year Group and Class: _____

Date: _____

Time: _____

Reason for investigation, cause for concern:

Please give this to the Designated Online Safety Lead, or a member of the Online Safety Group

Where a child is at risk of harm, this information must also be shared with the Designated Safeguarding Officer

Name and signature of person raising concern: _____

This information was passed to: _____ Date: _____ Time _____

Details of first reviewing person	Details of first reviewing person
Name: _____	Name: _____
Position: _____	Position: _____
Signature: _____	Signature: _____

Name and location of computer used for review: (Home or school device).(SEcurus log/information search

Reason for concern

Web site(s) address/device	
Conclusion and Action Proposed or Action Taken	

Recording Incidents of Online Safety - responding to incidents of misuse

Reporting Log – a record of Online Safety Incidents						
Date	**Time**	**Incident**	**Action Taken**		**Incident Reported By**	**Signature**
			What?	**By Whom?**		
		Pupil name-				
		Pupil name-				
		Pupil name-				
		Pupil name-				
		Pupil name-				
		Pupil name-				
		Pupil name-				