Padiham Green CE Primary School

Jesus said, "Come, follow me." Matthew 4:19

Online Safety Policy

Review of this Policy: This policy will be reviewed annually by the Governing Board

Revised: May 2025

Curriculum Intent

By living and learning through God, we strive to provide a secure and stimulating environment where the children enjoy school and demonstrate a desire to learn. Through the delivery of an exciting, engaging and broad curriculum, we strive to achieve the highest standards and seek to develop the full potential of every child.

As a Church of England School, we are committed to fostering Christian values and beliefs. Through God's love and guidance, our ethos is embedded in the vision of the school and underpinning all aspects of school life at Padiham Green CE Primary School is the vision statement: Jesus said, "Come, follow me." (Matthew 4:19).

We want our children to **LOVE**, to **LEARN** and to **SHINE** on their journey at Padiham Green.

Padiham Green is a Christian school where everyone is valued. As a school family, we set good examples to all our learners following the examples set by Jesus. Using gospel values of **LOVE - FAITH – HOPE – THANKFULNESS - RESPECT – FORGIVENESS** we guide everyone along the right path, so that they may experience 'Life in all its fullness'.

Padiham Green Primary School understands that using online services is an important aspect of raising educational standards, promoting pupil achievement and enhancing teaching and learning. The use of online services is embedded throughout the school; therefore, there are a number of controls in place to ensure the safety of pupils and staff.

The purpose of this policy

The purpose of this policy is to:

- Ensure the safety and wellbeing of children and young people is paramount when adults, young people or children are using the internet, social media or mobile devices;
- Provide staff, parent and volunteers with the overarching principles that guide our approach to online safety;
- Ensure that, as an organisation, we operate in line with our values, and within the law, in terms of how we use online devices.

Scope of the Policy

This policy applies to all members of the Padiham Green C E Primary School community (including staff, pupils, volunteers, parents, carers, visitors) who have access to, and are users of, school digital technology systems, both in and out of Padiham Green C E Primary School. The Education and Inspections Act 2006 empowers headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of online bullying, or other online safety incidents covered by this policy, which may take place outside of Padiham Green C E Primary School but is linked to pupils of this school. The 2011 Education

Act increased these powers with regard to the searching for, and of, electronic devices, and the deletion of data. In the case of both acts, action can only be taken over issues covered by the school's behaviour policy.

Padiham Green C E Primary School will deal with such incidents within the online learning policy, the behaviour policy and the anti-bullying policy and will, where known, inform parents and carers of incidents of inappropriate online safety behaviour that take place out of school.

Our vision for eSafety

The school provides a diverse, balanced and relevant approach to the use of technology. Children are encouraged to maximise the benefits and opportunities that technology has to offer. The school ensures that children learn in an environment where security measures are balanced appropriately with the need to learn effectively. Children are equipped with the skills and knowledge to use technology appropriately and responsibly. They are taught how to recognise the risks associated with technology and how to deal with them, both within and outside the school environment. All users in the school community understand why there is a need for an Online Safety Policy.

Roles and Responsibilities

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

Headteacher

The headteacher and senior leaders:

- Have a duty of care for ensuring the safety (including online safety) of members of the school community;

- 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 or pupils;

- Are responsible for ensuring that relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant;

- 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. This is to provide a safety net and also support to those colleagues who take on important monitoring roles;

- Take day to day responsibility for online safety issues and have a leading role in establishing and reviewing the school online safety policies and documents;

- Receive reports of online safety incidents and create a log of incidents to inform future online safety developments.

Designated Safeguarding Lead

The DSL is trained in online safety issues and is aware of the potential for serious child protection and safeguarding issues to arise from:

- Sharing of personal data

- Access to illegal and/or inappropriate materials

- Inappropriate online contact with adults or strangers

• Potential or actual incidents of grooming

• Online bullying

• Sexting

They will:

- Hold the lead responsibility for online safety, within their safeguarding role.
- Receive relevant and regularly updated training in online safety to enable them to understand the risks associated with online safety and be confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online.
- Meet regularly with the online safety governor to discuss current issues, review (anonymised) incidents and filtering and monitoring logs and ensuring that annual (at least) filtering and monitoring checks are carried out.
- Attend relevant governing body meetings/groups.
- Be responsible for receiving reports of online safety incidents and handling them, and deciding whether to make a referral by liaising with relevant agencies, ensuring that all incidents are recorded.
- Liaise with staff and IT providers on matters of safety and safeguarding and welfare (including online and digital safety).
- Receive reports of online safety issues, being aware of the potential for serious child protection concerns and ensure that these are logged to inform future online safety developments. The

The DSL and Computing Curriculum lead will:

- 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.
- Provide (or identify sources of) training and advice forstaff/governors/parents/carers/learners.
- Receive regularly updated training to allow them to understand how digital technologies are used and are developing (particularly by learners) with regard to the areas defined In Keeping Children Safe in Education:

    - Content
    - Contact
    - Conduct
    - Commerce

Teaching and Support Staff
Teachers and teaching 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 policy/agreement (AUP/AUA) as well as the school's social media policy.
• They report any suspected misuse or problem to the headteacher for investigation;
• All digital communications with pupils, parents and 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;
• Pupils understand and follow the Online Safety Policy and acceptable use policies;
• Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations;

- They monitor the use of digital technologies, mobile devices and cameras, 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.
- LCC approved filtering systems are securely in place for obstructing all access to unsuitable material during internet searches.

Curriculum Lead

Curriculum Leads will work with the DSL/OSL to develop a planned and coordinated online safety education programme.
This will be provided through:

- A mapped curriculum plan in computing lessons
- PHSE programmes
- Through relevant national initiatives and opportunities such as Safer Internet Day and Antibullying week.

Governors

Governors are responsible for reviewing the effectiveness of the policy. This will be carried out by the governors receiving regular information about online safety incidents and monitoring reports. The role of the governor will include:

- Regular monitoring of online safety incident logs
- Reporting to relevant Governors meetings regular meetings with the Designated Safeguarding Lead / Online Safety Lead
- Regularly receiving (collated and anonymised) reports of online safety incidents
- Checking that provision outlined in the Online Safety Policy (e.g. online safety education provision and staff training is taking place as intended)
- Ensuring that the filtering and monitoring provision is reviewed and recorded, at least annually. (The review will be conducted by members of the SLT, the DSL, and the IT service provider and involve the responsible governor) - in-line with the DfE Filtering and Monitoring Standards
- Receiving (at least) basic cyber-security training to enable the governors to check that the school meets the DfE Cyber-Security Standards

Network Manager/Technical staff

Those with technical responsibilities 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 all LCC online safety policy and guidance that may apply;
- That users may only access the networks and devices through a properly enforced password protection policy;
- The filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person;
- That they keep up to date with online safety technical information in order to carry out their online safety role effectively 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 headteacher or senior leaders for investigation/action/sanction;
- That monitoring software/systems are implemented and updated as agreed in school policies.

IT Provider

The IT Provider is responsible for ensuring that:

- They are aware of and follow the school Online Safety Policy and Technical Security Policy to carry out their work effectively in line with school police.
- The school technical infrastructure is secure and is not open to misuse or malicious attack.
- The school meets the required online safety technical requirements as identified by the DfE Meeting Digital and Technology Standards in Schools & Colleges and guidance from local authority.
- There is clear, safe, and managed control of user access to networks and devices.

- They keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant.
- The use of technology is regularly and effectively monitored in order that any misuse/attempted misuse can be reported to (insert relevant person) 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.

Pupils

Pupils are responsible for using the school digital technology systems in accordance with the pupil acceptable use agreement. They should:

- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations;
- Understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so;
- Be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand school policies on the taking of, or use of, images, and on online-bullying;
- 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 online learning or school activities.

Parents and carers

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

The breadth of issues classified within online safety is considerable, but they can be categorised into three areas of risk:

- Content: Being exposed to illegal, inappropriate or harmful material, e.g. pornography, fake news, and racist or radical and extremist views.
- Contact: Being subjected to harmful online interaction with other users, e.g. commercial advertising and adults posing as children or young adults.
- Conduct: Personal online behaviour that increases the likelihood of, or causes, harm,e.g. sending and receiving explicit messages, and cyberbullying.

The measures implemented to protect pupils and staff revolve around these areas of risk. Our school has created this policy with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all pupils and staff.

Policy Statements

Security and data management

IT security is a complex subject that involves all technology users in the school, dealing with issues regarding the collection and storage of data through to the physical security of equipment. The Lancashire IT Security Framework (published 2005) is consulted to ensure that procedures are in place to ensure data, in its many forms, is kept secure within the school. In line with the requirements of the Data Protection Act (2018), sensitive or personal data is recorded, processed, transferred and made available for access in school. This data is:

- Processed for limited purposes
- Processed in accordance with the data subject's rights
- Adequate, relevant and not excessive
- Kept no longer than necessary
- Only transferred to those when appropriate and who also have adequate protection
- Accessed, stored and disposed of by approved means if the data is confidential
- Password protected on all computers
- Not allowed to be removed from school premises without good reason

Managing the school website

- The school will ensure that information posted on the school website meets the requirements as identified by the Department for Education (DfE).
- The contact details on the website will be the school/setting address, email and telephone number. Staff or pupils' personal information will not be published.
- The head teacher will take overall editorial responsibility for online content published and will ensure that information is accurate and appropriate.
- The website will comply with the school's guidelines for publications including accessibility respect for intellectual property rights, privacy policies and copyright.
- The administrator account for the school website will be safeguarded with an appropriately strong password.
- The school will post information about safeguarding, including online safety, on the school website for members of the community.

Online learning

It is the duty of the school to ensure that every child in its care is safe. The same 'staying safe' outcomes and principles apply equally to the 'virtual' or digital world. ESafet is a partnership concern and is not limited to school premises, school equipment or the school day. This expectation also applies to anybody that makes use of the school's IT facilities and digital technologies. When learning online, pupils should adhere to the same code of conduct that they would follow during regular school lessons.

To ensure that e-learning takes place safely:

- Pupils and staff should keep their username and password safe and not share this with others.
- Learning platforms are monitored by staff and are only accessible to staff, pupils and parents of the school.
- E-Safety procedures that take place in school should continue at home where possible.
- Comments and messages should be appropriate and reflect conversations that would take place in school.
- Work is stored securely online and is only accessible by password.
- Any concerns should be raised immediately and passed on to the school's designated safeguarding lead (the headteacher).

Infrastructure and technology

Children's access and safe classroom use

Children are supervised at all times by a trusted adult when accessing school equipment and online material.

Children access the school systems through class logins which can only access certain areas of the network.

- The school's internet access will be designed to enhance and extend education.
- Access levels to the internet will be reviewed to reflect the curriculum requirements and the age and ability of pupils.
- All members of staff are aware that they cannot rely on filtering alone to safeguard children and supervision, classroom management and education about safe and responsible use is essential.
- Supervision of pupils will be appropriate to their age and ability.

- Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- The school will use age appropriate search tools (e.g. Google Safe Search or CBBC safe search), as decided by the school, following an informed risk assessment to identify which tool best suits the needs of our community.
- The school will ensure that the use of Internet-derived materials by staff and pupils complies with copyright law and acknowledge the source of information.
- Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- The evaluation of online materials is a part of teaching and learning in every subject and will be viewed as a whole-school/setting requirement across the curriculum.
- The school will use the internet to enable pupils and staff to communicate and collaborate in a safe and secure environment.

Managing the network and technical support

The school IT technician is responsible for managing the security of the school network and for installing all programmes. All wireless devices are security enabled and only accessible through a secure password. Appropriate settings have been appointed on tablet devices to restrict downloading of apps or in app purchases. All staff members have an individual log in and password whereas children have class logins. All staff members and children are reminded to log out of the school system when leaving a computer or device unattended.

Managing email

- Pupils may only use school/setting provided email accounts for educational purposes.
- All members of staff are provided with a specific school/setting email address to use for any official communication.
- The forwarding of any chain messages/emails etc. is not permitted. Spam or junk mail will be blocked and reported to the email provider.
- Any electronic communication which contains any content which could be subject to data protection legislation (e.g. sensitive or personal information) will only be sent using secure and encrypted email. Access to school /setting email systems will always take place in accordance to data protection legislation and in line with other appropriate school/setting policies e.g. confidentiality.
- Members of the community must immediately tell a designated member of staff if they receive offensive communication and this will be recorded in the school safeguarding files/records.
- Staff will be encouraged to develop an appropriate work life balance when responding to email, especially if communication is taking place between staff and pupils and parents.
- Parents are asked not to contact teachers after 5pm through email.
- 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.
- The school will have a dedicated email for reporting wellbeing and pastoral issues. This inbox will be managed by designated and trained staff.
- School email addresses and other official contact details will not be used for setting up personal social media accounts.

Filtering and Monitoring

The school filtering and monitoring provision is agreed by senior leaders, governors and the IT Service Provider and is regularly reviewed (at least annually) and updated in response to changes in technology and patterns of online safety incidents/behaviours.

The school uses the LGfL filtering service, (See http://www.lancsngfl.ac.uk/lgfladvice/index.php for more details.) Staff are aware that they must contact the IT Technician for blocking and unblocking specific websites. The school will work with LCC and the Schools Broadband team or broad to ensure that filtering policy is continually reviewed.

• The school will have a clear procedure for reporting breaches of filtering which all members of the school community (all staff and all pupils) will be made aware of.
• If staff or pupils discover unsuitable sites, the URL will be reported to the School Designated Safeguarding Lead and will then be recorded and escalated as appropriate.
• The School filtering system will block all sites on the Internet Watch Foundation (IWF) list.
• Changes to the school filtering policy will be risk assessed by staff with educational and technical experience prior to any changes and where appropriate with consent from the Leadership Team.
• All changes to the school filtering policy will be logged and recorded.
• The Leadership Team will ensure that regular checks are made to ensure that the filtering methods selected are effective and appropriate. checks on the filtering and monitoring system are carried out by the IT Service Provider with the involvement of a senior leader, the Designated Safeguarding Lead and a governor, in particular when a safeguarding risk is identified, there is a change in working practice, e.g. remote access or BYOD or new technology is introduced e.g. using SWGfL Test Filtering
• Any material that the school believes is illegal will be reported to appropriate agencies such as the police or CEOP immediately.

Filtering

- The school manages access to content across its systems for all users and on all devices using the school's internet provision. The filtering provided meets the standards defined in the DfE Filtering standards for schools and colleges and the guidance provided in the UK Safer Internet Centre Appropriate filtering.
- Illegal content (e.g., child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation URL 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, recognising that no system can be 100% effective.
- There is a clear process in place to deal with, and log, requests/approvals for filtering changes (see Appendix for more details).
- Filtering logs are reviewed weekly and the Designated Safeguarding Lead is alerted to breaches of the filtering policy which are then logged alongside action taken.
- The school is taking action to install new software to filter all managed devices which will report on harmful content in real time and alert the DSL.
- The new software will also provide real time monitoring, alerting staff and the DSL to risks and prompt action. It will also track patterns of online behaviour.

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.
- Monitoring reports are urgently picked up, acted on and outcomes are recorded by the Designated Safeguarding Lead, all users are aware that the network (and devices) are monitored.
- 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.
- 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 may 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

Technical Security
The school technical systems will be managed in ways that ensure that the school meets recommended technical requirements:

- Responsibility for technical security resides with SLT who may delegate activities to identified roles. 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 IT service provider and will be reviewed, at least annually, by the SLT.
- Password policy and procedures are implemented. (consistent with guidance from the National Cyber Security Centre)
- The security of their username and password and must not allow other users to access the systems using their log on details.
- All users 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.
- All school networks and system will be protected by secure passwords. Passwords must not be shared with anyone.
- The administrator passwords for school systems are kept in a secure place.
- There is a risk-based approach to the allocation of learner usernames and passwords.
- 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
- 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 software.
- There are rigorous and verified back-up routines, including the keeping of network separated (air-gapped) copies off-site or in the cloud,
- The Headteacher is responsible for ensuring that all software purchased by and used by the school is adequately licenced 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).
- Use of school devices out of school and by family members is regulated by an acceptable use statement that a user consents to when the device is allocated to them.
- Personal use of any device on the school network is regulated by acceptable use statements that a user consents to when using the network.
- Staff members are not permitted to install software on a school-owned devices without the consent of the SLT/IT service provider.
- Removable media is not permitted unless approved by the SLT/IT service provider.
- Systems are in place to control and protect personal data and data is encrypted at rest and in transit.

Dealing with incidents

All members of the school community will be made aware of a number of online risks that are likely be encountered in a school setting. This will be highlighted within staff training and educational approaches for the pupils.

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 the incident must be escalated through the agreed school safeguarding procedures, this may include:

➢ Non-consensual images
➢ Self-generated images
➢ Terrorism/extremism
➢ Hate crime/ Abuse
➢ Fraud and extortion
➢ Harassment/stalking
➢ Child Sexual Abuse Material (CSAM)
➢ Child Sexual Exploitation Grooming
➢ Extreme Pornography
➢ Sale of illegal materials/substances
➢ Cyber or hacking offences under the Computer Misuse Act
➢ Copyright theft or piracy
➢ 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:

- internal response or discipline procedures
- involvement by local authority
- 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.
- 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 (as relevant and anonymously) to:

- the Online Safety Group for consideration of updates to policies or education programmes and to review how effectively the report was dealt with
- staff, through regular briefings
- learners, through assemblies/lessons
- parents/carers, through newsletters, school social media, website
- governors, through regular safeguarding updates
- local authority/external agencies, as relevant Illegal offences

Any suspected illegal material or activity must be brought to the immediate attention of the headteacher who must refer this to external authorities, for example, Police, CEOP, and Internet Watch Foundation (IWF). The school will never personally investigate, interfere with, or share evidence as it may inadvertently be committing an illegal offence. It is essential that correct procedures are followed when preserving evidence to protect those investigating the incident. Further information and procedures regarding specific incidents can be found in Appendix A.

Inappropriate use

It is more likely that school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with quickly and actions are proportionate to the offence.

Examples of inappropriate use include:
- Accidental access to inappropriate materials
- Using other people's logins and passwords maliciously
- Deliberate searching for inappropriate materials - bringing inappropriate electronic files from home
- Using chats and forums in an inappropriate way

Use of personal mobile phones and electronic devices

The widespread ownership of mobile phones and a range of other personal devices among children and adults will require school to take steps to ensure that mobile phones and personal devices are used responsibly. Although these devices are an accepted part of everyday life and can bring about many positive uses, they must be used appropriately in a school setting. These are valuable items that can be lost, stolen or damaged in the school environment and could also be considered as distracting or intrusive in a teaching or learning situation.

Pupil use of personal mobile phones and electronic devices
- The use of mobile phones by pupils is not permitted in school.
- Pupils should not bring mobile phones or electronic devices into school.
- If a pupil needs to contact his/her parents or carers they will be allowed to use a school phone or a member of the office staff will contact them on their behalf.
- Pupils will be instructed in safe an appropriate use of mobile phones and devices and will be made aware of boundaries or consequences.
- If a pupil breaches the school policy then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones or devices will be released to parents/carers at the end of the school day.
- School staff may confiscate a pupil's mobile phone or device if they believe it us being used to contravene the school's behaviour or bullying policy or could contain youth produced sexual imagery (sexting).
- If there is suspicion that material on a pupil's personal device or mobile phone may be illegal, or may provide evidence to a criminal offence, then the device will be handed over to the police for further investigation.

Staff use of personal mobile phone and devices

• Members of staff are not permitted to use their own personal phones or devices for contacting children, young people and their families within or outside of the setting in a professional capacity. Any pre-existing relationships which could compromise this will be discussed with leaders/managers. • Staff will not use personal devices such as mobile phones, tablets or cameras to take photos or videos of children and will only use work-provided equipment for this purpose.

• Staff will not use any personal devices directly with children and will only use work-provided equipment during lessons/educational activities.

• Members of staff will ensure that any use of personal phones and devices will always take place in accordance with the law e.g. data protection as well as relevant school policy and procedures e.g. confidentiality, data security, Acceptable Use etc.

• Staff personal mobile phones and devices will be switched off/switched to 'silent' mode during lesson times.

• Bluetooth or other forms of communication should be "hidden" or switched off during lesson times.

• Personal mobile phones or devices will not be used during teaching periods but may be left with the school office in the case of emergency circumstances when an urgent call is expected

• Staff will ensure that any content bought on site via mobile phones and personal devices are compatible with their professional role and expectations.

• If a member of staff breaches the school/setting policy then disciplinary action will be taken.

• If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal device or have committed a criminal offence then the police will be contacted.

• Any allegations against members of staff involving personal use of mobile phone or devices will be responded to following the school/settings allegations management policy.

Visitors' use of personal mobile phones and devices

• Parents/carers and visitors must use mobile phones and personal devices in accordance with the school's acceptable use policy.

• Adults in school must switch off mobile phones during school hours. Emergency calls may be made from the office only, at break times.

• Children are not allowed mobile phones under any circumstances.

• School related images, video or audio must not be recorded on a personal mobile phone.

• Parents are not allowed to video school shows and performances.

• Parents must not take group pictures at school events without written permission from parents and explicit permission from the headteacher. • Any photographs taken must not be uploaded to social media websites.

• Staff are fully aware of the potential for mobile phones to be used for cyberbullying.

• Staff will be vigilant in monitoring visitors for any covert use of mobile phones or cameras and report any suspicious use of mobile phones to a member of the SLT.

• Use of mobile phones or personal devices by visitors and parents/carers to take photos must take place in accordance with the school image use policy.

• Staff will be expected to challenge concerns when safe and appropriate and will always inform the Designated Safeguarding Lead of any breaches of use by visitors.

Use of digital media

The school has written consent from parents for photographs of their children to be taken or used. Students or visitors, not directly employed by the setting, are expressly forbidden to take photos to include in portfolios.

Taking Photographs / Video

Photographs and videos are only taken using school owned equipment and by staff employed by school. The use of personal equipment to store images is forbidden. When taking photographs, staff ensure that children are respected and that photographs do not show children who are distressed or injured. Children will always be appropriately dressed and all staff members are aware of suitable and unsuitable locations.

- The school may use live-streaming or video-conferencing services in line with national and local safeguarding guidance / policies.

- 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.
- Learners' full names will not be used anywhere on the website in association with photographs.
- Written 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. Permission is not required for images taken solely for internal purposes.

Storage of Photographs / Video

Storage of visual images must be stored on the Teachers drive accessed only on school owned computers through a teacher log in. Photographs and videos are not stored on USB memory sticks or personal mobile devices. Images and videos taken on school owned mobile devices (for example, iPads) are swiftly uploaded to the main server before being deleted from the mobile device. Images should not be stored on mobile devices. Staff must not store images on personal equipment nor are they allowed to store personal images on school equipment. All staff understand how to dispose of printed images in the appropriate way. Videos and photographs that are submitted as part of online assignments will be stored securely on the school's server.

Video Conferencing

When video conferencing is used, children, staff and parents will be reminded to uphold good standards of behaviour and follow the guidance of the organiser of the call. Video conferencing sessions will be held through secure platforms (Zoom and Microsoft teams) and are to not be recorded.

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 to see how data recorded, processed, transferred, disposed and made available).
- Implements the data protection principles and can demonstrate that it does so. 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 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.
- 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.

- 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.

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 digital literacy 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.

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities, and will be provided in the following ways:

- A planned online safety curriculum for all year groups matched against a nationally agreed framework, the SWGfL Project Evolve, and is 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; 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.
- Vulnerability is actively addressed as part of a personalised online safety curriculum e.g., for victims of abuse and SEND.
- Key online safety messages should be reinforced as part of whole school activities.
- Pupils should be taught in all lessons to be critically aware of the materials and 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 and to respect copyright when using material 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.
- Staff should act as good role models in their use of digital technologies.
- In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use; LCC filtering processes are in place for blocking all unsuitable material and content.
- The online safety education programme should be relevant and up to date to ensure the quality of learning and outcomes.

Engagement and education of children considered to be vulnerable

- School is aware that some children may be considered to be more vulnerable online due to a range of factors.
- School will ensure that differentiated and ability appropriate online safety education is given, with input from specialist staff as appropriate.

Engagement and education of staff

- The online safety policy will be formally provided to and discussed with all members of staff as part of induction and will be reinforced and highlighted as part of our safeguarding responsibilities.
- Staff will be made aware that our Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential when using school systems and devices.

• Up-to-date and appropriate staff training in safe and responsible Internet use, both professionally and personally, will be provided for all members of staff in a variety of ways, on a regular basis.
• All members of staff will be made aware that their online conduct out of school could have an impact on their role and reputation within school. Civil, legal or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.
• The school/setting will highlight useful online tools which staff should use according to the age and ability of the pupils.

Parents/carers
Parents and carers may only have a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring and regulation of the children's online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond. The school will therefore seek to provide information and awareness to parents and carers through:

• Curriculum activities
• Letters, newsletters and the school website.
• Parents'/carers' evenings and online safety workshops and sessions.

<u>Outcomes</u>

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 produced by Martin Simpson and Lisa Tyrer

Appendix A

Procedures for Responding to Specific Online Incidents or Concerns

Responding to concerns regarding Youth Produced Sexual Imagery or "Sexting"

• School views "sexting" as a safeguarding issue and all concerns will be reported to and dealt with by the Designated Safeguarding Lead.

• If the school are made aware of incident involving creating youth produced sexual imagery the school will:

- Act in accordance with the school's child protection and safeguarding policy and the relevant safeguarding procedures.
- Immediately notify the designated safeguarding lead. - Store the device securely.
- Carry out a risk assessment in relation to the children(s) involved. - Consider the vulnerabilities of children(s) involved (including carrying out relevant checks with other agencies)
- Make a referral to children's social care and/or the police (as needed/appropriate).
- Put the necessary safeguards in place for children e.g. offer counselling support and immediate protection and offer appropriate pastoral support for those involved.
- Implement appropriate sanctions in accordance with the school's behaviour policy but taking care not to further traumatise victims where possible.

- Inform parents/carers about the incident and how it is being managed.
• The school will not view an image suspected of being youth produced sexual imagery unless there is no other possible option or there is a clear need or reason to do so (in these cases the image will only be viewed by the Designated Safeguarding Lead).
• The school will not send, share or save content suspected to be an indecent image of children and will not allow or request children to do so.
• If an indecent image has been taken or shared on the school/settings network or devices then the school will take action to block access to all users and isolate the image.
• The school will take action regarding the creation of youth produced sexual imagery, regardless of the use of school/setting equipment or personal equipment, both on and off the premises.

Responding to concerns regarding Online Child Sexual Abuse and Exploitation

• School will ensure that all members of staff are made aware of online child sexual abuse, including exploitation and grooming including the consequences, possible approaches which may be employed by offenders to target children and how to respond to concerns.
• The school will implement preventative approaches for online child sexual abuse via a range of age and ability appropriate educational approaches for pupils, staff and parents/carers.
• School views online child sexual abuse as a safeguarding issue and all concerns will be reported to and dealt with by the Designated Safeguarding Lead.
• If the school are made aware of an incident involving online child sexual abuse of a child then the school will:
- Act in accordance with the schools child protection and safeguarding policy. Immediately notify the designated safeguarding lead.
- Store any devices involved securely.
- Immediately inform the police via 101 (using 999 if a child is at immediate risk)
- Where appropriate the school will involve and empower children to report concerns regarding online child sexual abuse e.g. using the Click CEOP report form: www.ceop.police.uk/safetycentre/ Carry out a risk assessment which considers any vulnerabilities of pupil(s) involved (including carrying out relevant checks with other agencies).
- Make a referral to children's social care (if needed/appropriate).
- Put the necessary safeguards in place for pupil(s) e.g. offer counselling support and immediate protection and offer appropriate pastoral support for those involved.
- Inform parents/carers about the incident and how it is being managed.
- Review the handling of any incidents to ensure that the school is implementing best practice and the school leadership team will review and update any management procedures where necessary.
• The school will take action regarding online child sexual abuse regardless of the use of school equipment or personal equipment, both on and off the school premises.
• The school will ensure that all members of the community are aware of sources of support regarding online child sexual abuse.

Responding to concerns regarding Indecent Images of Children (IIOC)

• The school will take action in regard of Indecent Images of Children (IIOC) regardless of the use of school/setting equipment or personal equipment, both on and off the premises.
• The school will take action to prevent access, or accidental access, to Indecent Images of Children (IIOC) for example using an internet Service provider (ISP) which subscribes to the Internet Watch Foundation block list, implementing appropriate web filtering, implementing firewalls and anti-spam software.
• If the school is unclear if a criminal offence has been committed, then the Designated Safeguarding Lead will obtain further advice immediately.
• If the school/setting is made aware of Indecent Images of Children (IIOC) then the school will:
- Act in accordance with the schools child protection and safeguarding policy and immediately notify the school Designated Safeguard Lead.

- Store any devices involved securely.
- Immediately inform appropriate organisations
 • If the school are made aware that a member of staff or a pupil has been inadvertently exposed to indecent images of children whilst using the internet then the school will:
- Ensure that the Designated Safeguard Lead is informed. Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk
- Ensure that any copies that exist of the image, for example in emails, are deleted.
• If the school are made aware that indecent images of children have been found on the schools electronic devices then the school will:
 - Ensure that the Designated Safeguard Lead is informed.
- Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk
- Ensure that any copies that exist of the image, for example in emails, are deleted. Inform the police via 101 (999 if there is an immediate risk of harm) and children's social services (as appropriate).
- Only store copies of images (securely, where no one else has access to them and delete all other copies) at the request of the police only.
• If the school are made aware that a member of staff is found in possession of indecent images of children on their electronic device provided by the school, then the school will: - Ensure that the Designated Safeguard Lead is informed or another member of staff in accordance with the school whistleblowing procedure.
- Contact the police regarding the images and quarantine any devices involved until police advice has been sought.
- Inform the Local Authority Designated Officer (LADO) and other relevant organisations in accordance with the schools managing allegations policy.
- Follow the appropriate school policies regarding conduct.

Responding to concerns regarding radicalisation and extremism online

• The school will take all reasonable precautions to ensure that children are safe from terrorist and extremist material when accessing the internet in schools and that suitable filtering is in place which takes into account the needs of pupils.
• When concerns are noted by staff that a child may be at risk of radicalisation online then the Designated Safeguarding Lead (DSL) will be informed immediately, and action will be taken in line with the safeguarding policy.
• Online hate content directed towards or posted by specific members of the community will be responded to in line with existing school policies, including anti-bullying, behaviour etc. If the school is unclear if a criminal offence has been committed, then the Designated Safeguarding Lead will obtain advice immediately Responding to concerns regarding cyberbullying
• Cyberbullying, along with all other forms of bullying, of any member of School community will not be tolerated. Full details are set out in the school policies regarding anti-bullying and behaviour. • All incidents of online bullying reported will be recorded.
• There are clear procedures in place to investigate incidents or allegations and support anyone in the school community affected by online bullying.
• If the school is unclear if a criminal offence has been committed then the Designated Safeguarding Lead will obtain advice immediately.
• Pupils, staff and parents/carers will be advised to keep a record of cyberbullying as evidence.
• The school will take steps to identify the bully where possible and appropriate. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.

Responding to concerns regarding online hate

• Online hate at school will not be tolerated.

- All incidents of online hate reported to the school will be recorded.
- All members of the school community will be advised to report online hate in accordance with relevant school policies and procedures e.g. anti-bullying, behaviour etc.
- The Police will be contacted if a criminal offence is suspected. If the school is unclear if a criminal offence has been committed then the Designated Safeguarding Lead will obtain advice as outlined in the safeguarding policy.

Appendix B

Online Safety (e-Safety) Contacts and References

National Links and Resources Action

Fraud: www.actionfraud.police.uk

BBC WebWise: www.bbc.co.uk/webwise

CEOP (Child Exploitation and Online Protection Centre): www.ceop.police.uk

ChildLine: www.childline.org.uk

Childnet: www.childnet.com

Get Safe Online: www.getsafeonline.org

Internet Matters: www.internetmatters.org

Internet Watch Foundation (IWF): www.iwf.org.uk

NSPCC: www.nspcc.org.uk/onlinesafety

Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline

Think U Know: www.thinkuknow.co.uk

UK Safer Internet Centre: www.saferinternet.org.uk