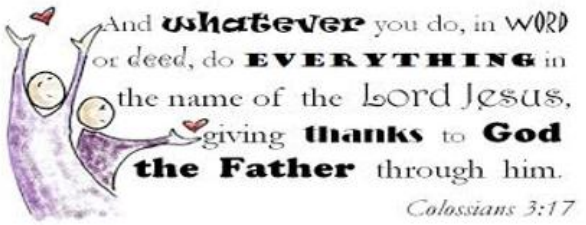
Online Safety and Acceptable Use Policy
Medlar with Wesham C of E Primary School



Our Christian Vision Mission Statement

We are a loving, caring, distinctively Christian family, providing an excellent education in a safe, happy environment, where every individual is valued as a child of God.

Policy Adapted: September 2025
Policy Adopted by the Governing Body: November 2025
Policy Review Date: September 2026

Vision:

By reflecting the principles of the Christian Faith at Medlar with Wesham Church of England Primary School we aim to celebrate the uniqueness of each child and through high expectations enable all our children to reach their full potential and become happy, confident and successful individuals.

Policy Overview:

Appendices:

Section 1- Medlar with Wesham Church of England Primary School Vision for Computing and Online Safety.

1.1 Our Statement of Intent

Preparing our pupils for the digital world; unlocking the potential

Technology is changing the lives of everyone. Through teaching Computing we equip children to participate in a rapidly-changing world where work and leisure activities are increasingly transformed by technology.
It is our intention to enable children to find, explore, analyse, exchange and present information. We also focus on developing the skills necessary for children to be able to use information in a safe and effective way. We want children to know more, remember more and understand more in computing so that they leave primary school computer literate.

1.2 Effective Practice

The use of IT in the current curriculum is vital, yet it is vital that our children and staff are aware, prepared and informed about using the internet and computer systems safely and constructively. Online Safety depends on effective practice at a number of levels and we achieve this by:

- Modelling responsible use of IT by ALL staff including outside of the school setting
- Encouraging children to maximise the benefits that technology can offer them

- Sound implementation of the Online Safety Policy with all staff including; support staff, administrative staff and Governors.
- Safe and secure broadband from a trusted and evaluated provider to provide an effective management of web filtering and monitoring
- Ensuring that Online Safety is taught each half term by members of staff
- Supporting parents with advice for online safety at home
- Ensuring that the Online Safety Leader and DSLs (when appropriate) receive up to date training when required.

Section 2- Teaching and Learning

2.1 Why is the internet so important?

The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils. Pupils use the Internet widely outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security. The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions.

2.2 How does Internet Use Benefit Learning?

The effective use of ICT has been found to provide huge benefits for pupils. Teachers and pupils will have access to a range of websites offering valuable educational resources, news and current events. This will provide opportunities for discussion, debate and higher-level independent learning. The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils. Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of pupils.
Staff should guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity. Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

2.3 Pupils will be taught how to evaluate Internet content

The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law. Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy. Pupils will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work. The evaluation of on-line materials is a part of every subject. Pupils should be taught research techniques including the use of subject catalogues and search engines and be encouraged to question the validity, currency and origins of information. Key information handling skills include establishing the author's name, date of revision and whether others link to the site. Pupils should compare web material with other sources. Effective guided use will also reduce the opportunity pupils have for exploring unsavoury areas. The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
Pupils should be taught to be critically aware of the materials they read and shown how to validate

information before accepting its accuracy.

2.4 Preventing Extremism

The internet is a powerful tool to target new people in order to indoctrinate them. Radicalisation is the promotion of increasingly extreme political, social or religious ideals. Extremism presents distorted views of history, politics or religion through persuasive narratives.
Pupils, through rigorous Online safety education and the measures previously described in section (2.3) of this policy should be empowered to challenge ideas, think critically for themselves and take responsibility for their actions. Related issues should be considered in the context of a balance PSHE curriculum.

Section 3- Responsibilities

3.1 Online Safety Related Issues:

For Online Safety to be effective, we expect all members of staff in school to take responsibility for maintaining this policy as it is their duty of care. This includes the safe and appropriate use of technology by staff and pupils.
The Headteacher, DSLs and Computing Leader are the main points of contact for online safety related issues and incidents.

Responsibilities include:

- Operational responsibility for ensuring the development, maintenance and review of the school's Online Safety Policy and associated documents, including Acceptable Use Policies.
- Ensuring that the policy is implemented and that compliance with the policy is actively monitored.
- Ensuring all staff are aware of reporting procedures and requirements should an online safety incident occur.
- Ensuring an Online Safety Incident Log is appropriately maintained and regularly reviewed.
- Keeping personally up-to-date with online safety issues and guidance through liaison with the Local Authority and through advice given by national agencies such as the Child Exploitation and Online Protection Centre (CEOP).
- Providing or arranging online advice/training for staff, parents/carers and governors.
- Ensuring the Headteacher, SLT, staff, children and governors are updated as necessary.
- To ensure a co-ordinated approach across relevant safeguarding areas with other safeguarding leads.

3.2 Headteacher

- The Head teacher and Deputy Head who is also a DSL, are aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. (See appendix 6)
- The Head teacher and Senior Leaders are responsible for ensuring that the online safety leader and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.

3.3 Technical Staff

- Technical support is provided by Lancs ICT LTD.

- Meets regularly with the Computing/ Online Safety Leader to discuss online safety issues.
- The technical staff are aware of the Online Safety Policy and Acceptable Use Policy.
- Ensures that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- Ensures that the school meets required online safety technical requirements and any Local Authority / other relevant body online safety policy or guidance applies.
- Ensures that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed 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.

3.4 Governors

Governors are responsible for the approval of the online safety policy and for reviewing the effectiveness of the policy. This will be carried out by the Governor panel receiving regular information about online incidents and monitoring reports. A member of the Governing Body has taken on the role of online safety Governor.

The role of the online safety Governor will include:

- Regular meetings with the online safety leader
- Regular monitoring of online safety incident logs
- Regular monitoring of filtering / change control logs
- Reporting to relevant Governors / Board / committee meeting

3.5 Teachers and Support Staff

Teaching and support staff are responsible for ensuring that:

- They have an up to date awareness of online safety and current trends
- They have an awareness of the current online safety policy and practices.
- They have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP)
- They report any suspected misuse or problems to the Head teacher or the Online Safety Leader
- All digital communications with students / pupils / parents / carers should be on a professional level and only carried out using official school systems
- Online safety issues are embedded in all aspects of the curriculum and other activities
- Ensure pupils in their care understand and follow the Online Safety Policy and Acceptable Use Policies when using technology and online communication methods.
- Ensure pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations

Monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement school rules of acceptable use 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 are in place for dealing with any unsuitable material that is found in internet searches

3.6 Designated Safeguarding Lead

The DSL should be trained in and actively maintain their own knowledge around online safety issues and be aware of current trend/ policies for Internet misuse and serious child protection / safeguarding issues that may arise from:

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

3.7 Pupils

- Responsible for using the school digital technology systems in accordance with the Student / Pupil Acceptable Use Policy
- Primarily need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- Need to understand the importance of reporting abuse, misuse or 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 forms of collaborating online. They should also know and understand policies on the taking / use of images and on cyber-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 related to their membership of the school.

3.8 Parents and 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. Medlar with Wesham Church of England Primary School will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, our website and information about national / local online safety campaigns and literature. Parents and carers will be encouraged to support the school in promoting good online practice and to follow guidelines on the appropriate use of different technologies.

Section 4 – Managing Internet Access

4.1 Appropriate and Safe Access to the Internet

The Internet is freely available to any person wishing to send e-mail or publish a website. In common with other media such as magazines, books and video, some material available on the Internet is unsuitable for pupils. Pupils in school are unlikely to see inappropriate content in books due to selection by publisher and teacher, and the school will take every practical measure to ensure that children do not encounter upsetting, offensive or otherwise inappropriate material on the Internet.

The following key measures have been adopted to help ensure that our pupils are not exposed to unsuitable material:

- Our Internet is provided by BT Lancashire Services and has a 'firewall' filtering system intended to prevent access to inappropriate material (Netsweeper)
- Google images and other search engines/ pop-ups are further controlled by the SSL filter to block unwanted imagery on webpages.
- Staff will check that the sites pre-selected for pupil use are appropriate to the age and maturity of pupils.
- Staff will be particularly vigilant when pupils are undertaking their own search and will check that children are using the agreed search engines and terms.
- Pupils will be taught to use e-mail and the Internet responsibly in order to reduce the risk to themselves and others. Each class has a class email which is the teachers' responsibility. Individual email can be accessed through the 'Purple Mash' VLE however only pupils and staff within school can be emailed and emails have to be checked before being sent.
- Agreed Online Safety Rules are displayed in the Computer Suite and should be referred to even if ICT is being used outside of this space.
- The Computing Subject Leader will monitor the effectiveness of the Internet access strategies through communication with all members of staff.
- The Headteacher and Computing Subject Leader will ensure that the policy is implemented effectively.
- Methods to quantify and minimise the risk of pupils being exposed to inappropriate material will be reviewed in consultation with colleagues from other schools and advice from the LEA, our I.S.P. (Internet Service Provider) and the DfE.

4.2 Reporting Incidents

In the event that an online safety incident occurs that contravenes the online safety policy or agreed AUP's, it is important that the protocol below will be followed (Appendix 7). It is important to distinguish between illegal and inappropriate use of ICT. All incidents will be logged in an online safety folder kept in the Headteachers office. A most important element of our online rules is that pupils will be taught to tell an adult immediately if they encounter any material that makes them feel uncomfortable. If there is an incident in which a pupil is exposed to offensive or upsetting material the school will wish to respond to the situation quickly and on a number of levels;

- If one or more pupils discover (view) inappropriate material our first priority will be to give them appropriate support. The pupil's parents/carers will be informed and given an explanation of the course of action the school has taken. The school aims to work with parents/carers/guardians to resolve any issues.
- If pupils discover unsuitable sites they will be taught to report it to an adult in school. The adult will then inform the Computing / Online Safety Leader via the online safety reporting folder located in the school office. The Computing leader will report the URL (address) and content to BT Lancashire Services.
- Children will only use the Internet during lesson time and will do so under the direction of the teacher
- Pupils are expected to play their part in reducing the risk of viewing inappropriate material by obeying the Rules of Responsible Internet Use, which they have designed to help protect them from exposure to Internet sites carrying offensive material. If pupils abuse the privileges of access to the Internet or use email facilities and fail to follow the rules they have been

taught, then sanctions consistent with the Behaviour Policy will be applied. This will involve informing parents/carers/guardians. Teachers may also consider whether access to the Internet may be denied for a period of time.

4.3 Illegal Offences

Any suspected illegal material or activity must be brought to the immediate attention of the Head teacher who must refer this to external authorities, e.g. Police, CEOP, Internet Watch Foundation (IWF). Never personally investigate, interfere with or share evidence as you may inadvertently be committing an illegal offence. It is essential that correct procedures are followed when preserving evidence to protect those investigating the incident (See Appendix 6) Always report potential illegal content to the Internet Watch Foundation (http://www.iwf.org.uk).They are licensed to investigate – schools are not.

Examples of illegal offences are:

- Accessing child sexual abuse images
- Accessing non-photographic child sexual abuse images
- Accessing criminally obscene adult content
- Incitement to racial hatred

More details regarding these categories can be found on the IWF website - http://www.iwf.org.uk.

4.4 Inappropriate Use and Sanctions

It is important that any incidents are dealt with quickly and actions are proportionate to the offence. If the guidelines or AUPs are breached, or suspected of being breached, the Headteacher should be notified if appropriate. Some examples of inappropriate incidents are listed below with possible sanctions, although this will ultimately be at the discretion of the Headteacher. All incidents should be logged in the online safety incident log.

Where staff are suspected of contravening the AUP, this should be reported to the Headteacher who will take appropriate steps in accordance with the school's discipline policy. Our Lady and St Edward's uses a holistic approach to online safety, and as such all staff are responsible for dealing with online safety incidents appropriately at class level. The online champion should be notified of any online safety incidents, who will then liaise with the Headteacher as appropriate. The online safety log book will be kept securely in the Headteacher's office. This will be monitored regularly, with action plans put in place as necessary to avoid further incidents where possible.

Procedure and Sanction suggestions from Lancashire County Council (LA)

Incident	Procedure and Sanctions
Accidental access to inappropriate materials.	• Minimise the webpage/turn the monitor off/click the 'Hector Protector' button. • Tell a trusted adult. • Enter the details in the Incident Log and report to LGfL filtering services if necessary. • Persistent 'accidental' offenders may need further disciplinary action.
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.	• Inform SLT or designated eSafety Champion. • Enter the details in the Incident Log. • Additional awareness raising of eSafety issues and the AUP with individual child/class. • More serious or persistent offences may result in further disciplinary action in line with Behaviour Policy. • Consider parent/carer involvement.

We may choose to implement at the discretion of the following members of staff: Headteacher, DSLs, Computing Lead, Family Support worker or Learning Mentor.

4.5 Security and Data Management

We are aware that connection to the Internet significantly increases the risk that a computer or a computer network may be infected by a virus or accessed by unauthorised persons.

The IT technician will up-date virus protection regularly (Sophus provided by LCC), and both the technician and Computing leader will keep up-to-date with IT news, developments and work with the Internet Service Provider to ensure system security strategies to protect the integrity of the network are reviewed regularly and improved as and when necessary.

ICT security is a complex subject that involves all technology users dealing with issues regarding the collection and storage of data through to the physical security of equipment. The Lancashire ICT Security Framework (published 2005) has been 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 (1998) and (GDPR guidance 2018), sensitive or personal data is recorded, processed, transferred and made available for access in school.

This data must be:

- Accurate
- Secure
- Fairly and lawfully processed
- Processed for limited purposes
- Processed in accordance with the data subject's rights
- Adequate, relevant and not excessive
- Kept no longer than is necessary
- Only transferred to others with adequate protection.

In our school, data is kept secure and all staff are informed as to what they can/cannot do with regard to data in the following ways:
Key information is held on the school's Server accessed through password protection.
As part of the Induction process for new staff or procedures for staff changing roles individuals are updated on the location of data specifically required for their role.

Induction also confirms the sensitive and confidential nature of all data held.

Any data taken from the school environment is held on password protected or encrypted devices such as laptops or pen drives. We do not permit the use of Pen drives or Portable Hard Drives to transfer or hold any data. All staff are required to read, sign and return the school's Acceptable Use Policy. Staff understand that they should only use approved means to access, store and dispose of confidential data. Expectations regarding the use of mobile devices in school are made clear in the, Safeguarding Policy and the AUP's. We recommend that staff password protect their own mobile devices. Data stored on the administration server is backed up BT Lancashire Services as part of a subscription service. This is currently done nightly.

Section 5 - Infrastructure and Technology

5.1 Network

Medlar with Wesham Church of England Primary School aims to ensure that our infrastructure and network is as safe and secure as possible. This section of the policy defines the policies and procedures in place to safeguard users. The ICT network at MEDLAR WITH WESHAM is protected by a broadband filter. Our internet provider is BT Lancashire Services which includes a filtering service provided by Netsweeper. However, should unsuitable content not be detected by this filter, children are educated to minimise the screen and inform an adult immediately. They should also be educated to not close or turn off a computer as this may limit the technical support. Staff will subsequently report the URL of inappropriate content to LGFL via the online reporting form which is available in such an event. The school is also able to immediately block websites via the use of this filter and attempts to access any inappropriate content is flagged. This enables the school to block inappropriate material immediately at school level. An email may also be sent out to all staff to alert them to any threats if required.

5.2 Pupil Access

Children should only access the internet using school digital devices when directed by a member of staff. Any pupils seen with a piece of technology, schools or personal, will be challenged to why/what they are using the device for. Pupils should not be allowed to visit the Computing Suite without a responsible adult present.

5.3 Passwords:

1. Staff have passwords to access the teacher part of the server and these must not be shared.
2. Only staff user profiles will be able to make administrative changes to programmes and access the teachers' area of the network.
3. Pupils in EYFS will use a single, simple year group password for access to the school network. This profile will have limited privileges, with any changes reset upon logging out. Pupils in KS1 and KS2 will have their own personal username and password. This may be used for other apps and Ipads.
4. Passwords should be changed at least once every academic year.

5.4 Software/hardware:

- All software used in school must be owned by the school, or by staff at the school, with appropriate user licenses used.
- Licenses should be kept centrally in the designated License folder by the Bursar and reviewed annually with the Computing Leader (Matt Draper)
- App licences for volume app purchases are logged within the school iTunes account using the VPP system. (now known as Apple School Manager)
- Where appropriate, any annual subscriptions should be renewed in good time. This is the responsibility of the Computing Subject Leader and Bursar unless this is a subject or Key Stage specific App/ software, in which case the appropriate member of staff should be involved.
- All computing equipment and software is audited every 2 years at the same time as the computing policy is reviewed.
- Any additional equipment required will be budgeted for in the annual Action Plan.
- Software is installed on systems by the ICT technician or Matt Draper (Computing Lead)

5.5 Managing the Network and Technical Support:

The school network is managed by an ICT Company through a service level agreement. They are responsible for all aspects of network technical support and maintenance. The following procedures are to be followed to ensure the network and all data remains secure:

- Servers, wireless systems and cabling are securely located and physical access restricted Wireless devices must have security enabled.
- The wireless network is accessible only through a secure password, available only to IT members of Staff.
- The SLT and the Computing Subject Leader are responsible for managing the security of the school network.
- The safety and security of the network is reviewed by String on each maintenance visit.
- The Computing Subject Leader will also ensure measures are in place to maintain the security of the network where new risks arise.
- String ensure that all computers are configured to receive all necessary updates and patches.
- There is a separate password for pupils and staff, who each have their own user profile.
- Only staff will have permissions to change their system profile and install necessary software.
- The overall network administrator password is available only to the Computing Subject Leader and the Headteacher.
- Staff and pupils log out of computers at the end of each session.
- If any users suspect a breach of network security, they should inform the Computing/Online Safety Leader immediately.
- String and BTLancashire will be contacted for assistance.
- Removable storage devices are permitted to be used in school, however if they contain any sensitive data they must be in password-protected or encrypted folders.
- Removable storage devices are to be regularly checked for virus and this is the responsibility of the adult user.
- Where school laptops are loaned to teachers, these may be used for acceptable personal use only. Further guidance can be found in the 'Staff Use of Internet' AUP.
- String are aware of all requirements and standards regarding online safety.
- The Computing Subject Leader and Headteacher are responsible for liaising with and managing the technical support staff from String when using school computers.
- Logs are kept each visit to ensure essential maintenance has taken place.

5.6 Filtering and Virus Protection and Risk Evaluation:

Sophos Anti-Virus software is used on all school computers. This is updated regularly automatically by String. Any laptops or other devices that access the network must have up-to-date Anti-Virus software.

In accordance with; Keeping Children Safe in Education.

The school knows that Netsweeper is an appropriate filtering system that blocks illegal content and are IWF (Internet Watch Foundation) members since 2006. We have some control to permit access to specific content carefully checked by the class teacher and agreed by the Computing Subject Leader.

Medlar-with-Wesham CE currently assess our risk as low to medium therefore the majority of the monitoring approach will be physical. Where whole class teaching is taking place using digital

technology our risk assessment is considered medium risk due to the physical inability to monitor all screens at the same time. During these sessions, reminders about appropriate internet use and online safety will take place. Staff are aware of safe practice and understand the need to report any inappropriate use of the internet. The Online Safety Leader will keep up to date with monitoring advice and adjust school practice accordingly.

Section 6- Communication and Publishing

6.1 Email

Pupils will learn how to use e-mail and be taught e-mail conventions, children may be given personal e-mail addresses to use in school only- which is moderated by class teachers. Staff will use school e-mail address 'Office 365' to communicate with others, to request information and to share information. Each class has an e-mail address for shared class projects using Office 365.

It is important that communications with persons and organisations are properly managed to ensure appropriate educational use and that the good name of the school is maintained. Therefore:

- All staff will use Office 365 e-mail, which is the Lancashire preferred school email system.
- The Lancashire Grid for Learning Service will reduce the amount of SPAM and any SPAM incidents should be reported to the Westfield Centre.
- All users are aware of the risks of accessing content including SPAM, unsuitable materials and viruses from external email accounts, e.g. Hotmail or Gmail, in school. Personal email accounts should not be checked in the presence of children, or connected to the overhead projectors/whiteboards.
- All users are aware that email is covered by The Data Protection Act (1988) and the Freedom of Information Act (2000), meaning that safe practice should be followed in respect of record keeping and security.
- Any communication needed about children via e-mail will be done through initials and for appropriate reasons.
- The forwarding of chain letters is not permitted.
- Pupils will be taught that they must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- E-mail sent to an external organisation should be written carefully in the same way as a letter written on school headed paper.
- Teachers will endeavour to ensure that these rules remain uppermost in the pupil's minds when as they monitor children using e-mail.
- Pupils may send e-mail from a class e-mail account as part of planned lessons but will not be given individual e-mail accounts for external use.
- Pupils will have the e-mail messages they compose checked by a member of staff before sending them.
- Pupils will not have individual access to the class e-mail account.
- Pupils will have their own 'Class Dojo' and 'Seesaw' account which does allow for messaging/ commenting, however this will be conducted through a central account.

6.2 Published Content and the School Website

The school website is a valuable resource. It celebrates pupils' work, promotes the school and publishes resources for projects and homework. The website reflects the school's ethos, information

is accurately and well-presented and personal security is not compromised. Publication of information is considered from a security viewpoint as web sites can be accessed by anyone on the Internet.

- The contact details on the website are the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.
- All teachers have been trained in publishing on the website and are responsible for ensuring content is appropriate on class pages.
- The Head, Deputy Head, SLT, bursar and Computing Subject Leader will take overall editorial responsibility and ensure that content is accurate and appropriate.
- The website is a fundamental place for communicating online safety messages to pupils and parents/carers, and has a dedicated online safety section including a CEOP button for pupils
- All materials on the website shall adhere to copyright restrictions. - Sensitive documents should only be available in 'read-only' formats, such as PDFs.

6.3 Pupils' Images and Work

Photographs that include pupils add a liveliness and interest to the school's website that is difficult to achieve in any other way. Nevertheless the security of staff and pupils must come first. A check should be made that pupils in photographs are appropriately clothed.

- Photographs of pupils will not be published without parental permission.
- Photographs that include pupils will be selected carefully and will only enable individual pupils to be clearly identified when parental permission has been gained.
- Pupils' full names will not be used anywhere on the website.
- All parents, upon starting Medlar-with-Wesham CE, are asked to sign a consent form for use of their child's photo.
- The school will keep a record of all pupils who are not permitted to have their photos or work published to the web.
- The record will be kept up-to-date, for instance a child or family joins the school.
- It is up to the Parent/ carer of the child to inform the school of any changes of permission.

6.4 Cloud Storage

Medlar with Wesham Primary considers carefully where data is stored. We choose not to use a third party for server back up. Staff may use Microsoft OneDrive/TEAMS to store documents.

6.5 Social Networking and Personal Publishing

At Medlar with Wesham Primary we embrace the use of social media and teach the children to use it as a constructive platform. We will ensure that we provide them with the tools to help them use it safely. Nonetheless parents and teachers need to be aware that the Internet has emerging online spaces and social networks which allow individuals to publish unmediated content. Social networking sites can connect people with similar or even quite different interests. Guests can be invited to view personal spaces and leave comments, over which there may be limited control. For use by responsible adults, social networking sites provide easy to use, free facilities; although often advertising intrudes and may be dubious in content. Pupils should be encouraged to think about the ease of uploading personal information and the impossibility of removing an inappropriate photo or

address once published. To prevent our pupils accessing inappropriate social networking sites, the following procedures will be put in place:

- The school will block/filter access to social networking sites.
- Newsgroups will be blocked unless a specific use is approved.
- Pupils will be taught to never to give out personal details of any kind which may identify them or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and e-mail addresses, full names of friends, specific interests and clubs etc.
- Pupils and parents will be advised that the use of social networks is inappropriate for primary aged pupils and that they have minimum age restriction guidelines.
- When blogging in school children's names and pictures will not appear together.
- Blogging will be supervised at all times.
- Comments and responses will be monitored and checked before publishing.

Medlar with Wesham Primary considers the following to be an acceptable use of social media by staff;

- Staff must not give personal contact details to pupils or parents/carers including mobile telephone numbers, or details of any blogs or personal websites.
- Adults must not communicate with pupils using any digital technology where the content of the communication maybe considered inappropriate or misinterpreted.
- If a Social Network site is used by staff, details must not be shared with pupils and privacy settings be set at maximum.
- Staff should be aware that 'friends of friends' may be able to view 'tagged' photographs/comments, which may bring the individual member of staff or the school into disrepute.
- Comments made and photographs posted reflect the professional reputation of the school, and once posted cannot be un-done.
- Pupils must never be added as 'friends' by staff. If a pupil persists in making friend requests, it is necessary to log the incident in the online log and report to the online safety champion, who will deal with the matter appropriately.
- No pupils under the age of 13 should be encouraged to use Facebook. However, it is known that a large proportion of children under this age do use this Social Network. It is the school's responsibility to ensure that children are educated on the safe use of all Social Networks.
- All Medlar with Wesham Primary pupils will receive regular teaching and guidance in the safe use of the Internet, Emailing, Social Networking and Cyber-bullying. Key messages and learning will be delivered during specific computing cyber-bullying awareness lessons, and re-enforced in class and whole school assemblies. Regular reminders will be used in class when children are accessing the Internet.
- Teachers can select from a wide range of resources to support this learning.

6.6 Video Conferencing

At Medlar with Wesham Primary the following statements outline what we consider to be acceptable and unacceptable use of Video conferencing:

- Approval must be sought in advance from the Headteacher prior to video-conferencing taking place.
- Only secure, approved programs to be used for video conferencing.

- All pupils will be supervised when using video conferencing.
- Additional written consent should be sought for the use of video conferencing from parents/carers if they do not wish for their child to take part.
- It should be made clear to the receiver that no recordings may be taken without permission.
- Staff know how to terminate the video conference at any time and feel confident to run the session without support of IT teams.

Section 7 – Mobile Technologies

The use of mobile devices, including laptops, tablets, mobile phones, cameras and games consoles is commonplace in school. Whilst these can provide a flexible solution and offer a range of exciting opportunities to extend children's learning, their use poses challenges in terms of online safety. Many of these devices integrate functionality to take images, access the Internet and engage users in various methods of external communication. Here at Medlar with Wesham Primary each classroom has a teacher ipad. Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

7.1 Mobile Phones and Smart Watches: Staff Use

Staff should have their personal phones/smart watches out of sight (e.g. in a drawer, handbag or pocket) during working hours (unless being used in one of the circumstances stated below.)

Personal mobile phones should not be used in a space where children are present eg. classroom, playground (unless being used in one of the circumstances stated below.)

Use of personal mobile phones (inc. receiving/sending texts and emails) should be limited to non-contact time when no children are present e.g. in office areas, staff room, empty classrooms. (unless being used in one of the circumstances stated below.)

In the event of a staff member being concerned about a sick relative/dependent or awaiting a doctor/nurse consultation via mobile phone a discussion must be had with the headteacher to determine acceptable use.

Staff members may have their personal mobile phone switched on and in their pocket/bag during transition between sites, at the Community Centre, in Church and whilst on the school field/forest school area, in case of emergency to communicate with the school office staff/headteacher via their mobile phones.

Access to Teams during the school day for day to day communication purposes must be done primarily via school ipads/desk tops and laptops, if these are not available then mobile phone devices can be used.

All personal mobile phones are the responsibility of their owner and school accepts no responsibility if they are lost, damaged or stolen as these items are brought into the workplace at the owner's risk.

Children are not permitted to bring mobile phones into school unless this has been agreed between staff and parents for a specific purpose. In this instance the pupil's/family's phone will be stored in the class teacher's desk drawer at the child's own risk. Any pupil mobile phones are the

responsibility of their owner and school accepts no responsibility if they are lost, damaged or stolen as these items are brought into school at the owner's risk.

- If a mobile phone is brought into school by a pupil without permission it will be confiscated immediately and returned to the family at the end of the school day.
- Staff are encouraged to use their mobile phone as a safety control measure during school trips. However, school devices are to be used primarily for photography whenever possible.
- Through online safety awareness training and the computing curriculum staff and pupils are made aware of issues around cyber-bullying

7.2 Cameras and Recording Devices

The use of cameras and sound recording devices offer substantial benefits to education but equally present school with challenges particularly regarding publishing or sharing media on the Internet, e.g. on Social Network sites. Photographs and videos of children and adults may be considered as personal data in terms of The Data Protection Act (1998).

- No cameras or other recording devices (including iPads) are to be taken from the school site for personal use.
- No personal cameras can be used in school, this includes devices with a built in camera such as a mobile phone to photograph pupils.

7.3 Consent and Purpose

- Biannually the school asks parents agree to the Image consent agreement, they should respond to this if they DO NOT agree with it, otherwise Medlar with Wesham C of E Primary will assume permission. These are collated and permissions communicated to class teachers and club leaders in school.
- The consent of adult staff members to have their photographs taken is assumed unless told otherwise.
- The purpose of any photography is always communicated to those involved (ie. assessment, display, celebration, website, media).
- Visitors must ask consent to take photographs and act in accordance with relevant codes of conduct.

7.4 Taking Photographs / Video

- All adults in school are permitted to take photographs for school purposes at the direction of class teachers using school owned equipment whenever possible.
- If a child does not want to be photographed their choice will be respected. Children are not filmed or photographed when this might cause embarrassment, distress or if the child is injured.
- In addition, photography that could be misinterpreted is also avoided. E.g. close up shots of children participating in PE activities.
- Teachers will take a range of photographs representing many or all class members. - Group shots, with a background context are favoured.

7.5 Parents Taking Photographs/Videos

In line with our Safeguarding policy, Parents are asked not to take photographs during performances, which will then be uploaded to social media without parental consent. Under the Data Protection Act (1998), parents are entitled to take photographs of their own children on the provision that the images are for their own use, e.g. at sports day. At these events parents are reminded that images and video cannot be published on social networking sites.

7.6 Storage of Photographs / Video

- All images are stored on password protected school equipment. On rare occasions images may be taken off site for the purposes of producing a display; in these instances they are kept on the same password protected equipment and returned to school.
- Staff do not store images on personal equipment.
- Access to equipment containing images is managed and monitored by class teachers. It is also the class teachers' responsibility to delete and dispose of digital and printed video/images.
- Emailed images are sent within the school's secure email system but using the server is the preferred delivery route.
- Full names are never published with images.
- Photos can be saved in shared TEAMS folders.
- Photos will be deleted from the server/TEAMS after seven years although a small number of photos may be kept for curriculum evidence and to commemorate special events.

Section 8.

The use of Artificial Intelligence (AI) systems in School

As Generative Artificial Intelligence (gen AI) continues to advance and influence the world we live in, its role in education is also evolving. There are currently 3 key dimensions of AI use in schools: learner support, teacher support and school operations; ensuring all use is safe, ethical and responsible is essential.

We realise that there are risks involved in the use of Gen AI services, but that these can be mitigated through our existing policies and procedures, amending these as necessary to address the risks.

We will educate staff and learners about safe and ethical use of AI, preparing them for a future in which these technologies are likely to play an increasing role.

The safeguarding of staff and learners will, as always, be at the forefront of our policy and practice.

Policy Statements

•The school acknowledges the potential benefits of the use of AI in an educational context - including enhancing learning and teaching, improving outcomes, improving administrative processes, reducing workload and preparing staff and learners for a future in which AI technology will be an integral part. Staff are encouraged to use AI based tools to support their work where appropriate, within the frameworks provided below and are required to be professionally responsible and accountable for this area of their work.

•We will comply with all relevant legislation and guidance, with reference to guidance contained in Keeping Children Safe in Education and UK GDPR

•We will provide relevant training for staff and governors in the advantages, use of and potential risks of AI. We will support staff in identifying training and development needs to enable relevant opportunities.

•We will seek to embed learning about AI as appropriate in our curriculum offer, including supporting learners to understand how gen AI works, its potential benefits, risks, and ethical and social impacts. The school recognises the importance of equipping learners with the knowledge, skills and strategies to engage responsibly with AI tools.

•As set out in the staff acceptable use agreement, staff will be supported to use AI tools responsibly, ensuring the protection of both personal and sensitive data. Staff should only input anonymised data to avoid the exposure of personally identifiable or sensitive information.

•Staff will always ensure AI tools used comply with UK GDPR and other data protection regulations. They must verify that tools meet data security standards before using them for work related to the school.

•Only those AI technologies approved by the school may be used. Staff should always use school-provided AI accounts for work purposes. These accounts are configured to comply with organisational security and oversight requirements, reducing the risk of data breaches.

•We will protect sensitive information. Staff must not input sensitive information, such as internal documents or strategic plans, into third-party AI tools unless explicitly vetted for that purpose. They must always recognise and safeguard sensitive data.

•The school will ensure that when AI is used, it will not infringe copyright or intellectual property conventions – care will be taken to avoid intellectual property, including that of the learners, being used to train generative AI models without appropriate consent.

•AI incidents must be reported promptly. Staff must report any incidents involving AI misuse, data breaches, or inappropriate outputs immediately to the relevant internal teams. Quick reporting helps mitigate risks and facilitates a prompt response.

•The school will audit all AI systems in use and assess their potential impact on staff, learners and the school's systems and procedures, creating an AI inventory listing all tools in use, their purpose and potential risks. (Risk assessment matrices are attached as an appendix)

•We are aware of the potential risk for discrimination and bias in the outputs from AI tools and have in place interventions and protocols to deal with any issues that may arise. When procuring and implementing AI systems, we will follow due care and diligence to prioritise fairness and safety.

•The school will support parents and carers in their understanding of the use of AI in the school (this could be through an "AI in our school guide")

•AI tools may be used to assist teachers in the assessment of learners' work, identification of areas for improvement and the provision of feedback. Teachers may also support learners to gain feedback on their own work using AI

•Maintain Transparency in AI-Generated Content. Staff should ensure that documents, emails, presentations, and other outputs influenced by AI include clear labels or notes indicating AI

assistance. Clearly marking AI-generated content helps build trust and ensures that others are informed when AI has been used in communications or documents.

•We will prioritise human oversight. AI should assist, not replace, human decision-making. Staff must ensure that final judgments, particularly those affecting people, are made by humans and critically evaluate AI-generated outputs. They must ensure that all AI-generated content is fact-checked and reviewed for accuracy before sharing or publishing. This is especially important for external communication to avoid spreading misinformation.

•Recourse for improper use and disciplinary procedures. Improper use of AI tools, including breaches of data protection standards, misuse of sensitive information, or failure to adhere to this agreement, will be subject to disciplinary action as defined in Staff Disciplinary Policy.

Section 8 - Education and Training

8.1 Acceptable Use Policies (AUP)

Our Acceptable Use Policies are intended to ensure that all users of technology within school will be responsible and stay safe. It ensures that all users are protected from potential risk in their everyday use of ICT for educational, personal and recreational purposes. AUPs are recommended for Staff, Pupils and Visitors/Guests and must be signed and adhered to by users before access to technology is allowed. This agreement is a partnership between parents/carers, pupils and the school to ensure that users are kept safe when using technology. A list of children who, for whatever reason, are not allowed to access technology must be kept in school and made available to all staff. The school has the following AUP's in place (see appendices):

- Computing AUP – Staff and Governor Agreement
- Computing AUP – Supply Teacher and Visitors/Guests Agreement
- Computing AUP – Pupils Agreement/Online Safety Rules
- Computing AUP – Parent's letter

The school promotes online safety rules with ICT in teaching. These are displayed wherever computers are used in school. Education and training are essential components of effective online safety provision. Equipping individuals, particularly pupils, with the appropriate skills and abilities to recognise the risks and how to deal with them is fundamental. Online safety is embedded within the curriculum and advantages taken of new opportunities to promote online safety.

8.2 Online Safety Across the Curriculum

In 21st Century society, both adults and children need to be digitally literate and aware of the benefits that use of technology can provide. However, it is essential that children are taught to use technology responsibly, securely and safely, being able to recognise potential risks and knowing how to respond. They should, for example, be able to communicate safely and respectfully online, be aware of the necessity to keep personal information private, be taught how to search effectively and be discerning in their evaluation of digital content and be aware of the need to respect copyright and Intellectual Property rights. The three main areas of online safety risk (as mentioned by OFSTED, 2013) that school must be aware of and consider are:

- Children need to be taught that not all content is appropriate or from a reliable source. (A range of examples will be used with your child)
- Children need to be taught that contact may be made using digital technologies and that appropriate conduct is necessary when engaging with these technologies. (A range of examples will be used with your child)
- Children need to be made aware that their personal online behaviour can increase the likelihood of, or cause harm to themselves and others. (A range of examples will be used with your child)

Online safety is embedded in all ICT curriculum areas, in particular the strands of Information Technology and Digital Literacy. The school also participates in the annual 'Safer Internet Week', with specific teaching and discussion of online issues. The school is currently in the process of achieving the Online 360 award and has been awarded their first certificate. Other issues such as Cyber-bullying and 'Grooming' are discussed in PSHE sessions. The school online safety rules are regularly referenced during computing sessions. Where necessary, class teachers will differentiate their teaching to ensure all pupils remain safe when using technology. Pupils are also reminded of relevant legislation regarding the Internet, such as copyright implications. Pupils are taught during Digital Research units to critically evaluate materials and content. This is reinforced in all other cross-curricular ICT sessions. Online safety rules are displayed wherever computers are used in school. This is differentiated by key stage (see Appendices).

8.3 Raising Staff Awareness

- All staff, upon starting work at the school, are required to agree to the school's AUP's and are provided with a copy of the online safety policy and key staff guidelines, which includes personal safeguarding.
- Staff training updates for online safety will be delivered as necessary, with a minimum of once per academic year.
- All training and advice will be delivered by the, The Computing and Online Safety Leader.
- The Online Safety Leader will keep aware of updates to online safety guidelines and receive external training as necessary.
- All staff are expected to promote and model responsible use of ICT at all times, and all staff are responsible for promoting online safety whilst using ICT.

8.4 Raising Pupil Awareness

- Online safety rules will be displayed in all classrooms.
- Pupils will be informed that network and internet use will be monitored.
- An online safety module is included in all years of the PSHE and Computing Curriculum.
- Additional reference will be made to online safety during Online Safety day in February and during Anti Bullying week in November.
- Online safety rules are regularly referenced during all computing sessions.

8.5 Raising parents/carers awareness

"Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it." (Byron Report, 2008). At Medlar with Wesham Primary we offer

regular opportunities for parents/carers and the wider community to be informed about online safety, including the benefits and risks of using various technologies. This takes place through:

- School newsletters.
- A dedicated area on the school website, which promotes external online resources and online materials.
- We will communicate any online safety concerns highlighted from other sources such as the media.
- We will deliver any documentation from our cooperate support Vodafone and from Online Safety third party groups.

8.6 Raising Governor Awareness

- Governors are kept updated on arising online matters through the termly Curriculum Committee and Report to Governors for Computing.
- Governors also review and agree the Online Safety Policy annually.
- Governors sign the staff AUP

Medlar with Wesham Primary is committed to keeping children and staff safe online.

Appendix 1.

RE: Acceptable Use Policy (Pupils)

Pupil Acceptable Use Policy Agreement – for children

This is how we stay safe when we use computers:

- I will ask a teacher or suitable adult if I want to use the computers / tablets
- I will only use activities that a teacher or suitable adult has told or allowed me to use
- I will take care of the computer and other equipment
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong
- I will tell a teacher or suitable adult if I see something that upsets me on the screen
- I know that if I break the rules I might not be allowed to use a computer / tablet

Pupil Acceptable Use Policy Agreement

The school will try to ensure that pupils will have good access to digital technologies to enhance their learning and will, in return, expect the students / pupils to agree to be responsible users.

- I understand that my son / daughter will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

- I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

- I understand that my son's / daughter's activity on the systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

- I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's online safety.

Appendix 2.

ICT Acceptable Use Policy (AUP) Staff and Governors Agreement

ICT and the related technologies such as email, the Internet and mobile devices are an integral part of our daily life in school.

This agreement is designed to ensure that all staff are aware of their individual responsibilities when using technology. All staff members are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with (Headteacher).

1. I will take responsibility for my own use of any technologies, making sure that I use them safely, responsibly and legally.

2. I will be an active participant in online safety education, taking personal responsibility for my awareness of the opportunities and risks posed by the use of technology.

3. I will not use communications devices, whether school provided or personally owned, for bullying or harassment of others in any form.

4. I will not be involved with any online activities, either within or outside school that may bring the school, staff, pupils or wider members into disrepute. This includes derogatory/inflammatory comments made on Social Network Sites, Forums and Chat rooms.

5. I will not browse, download/upload or distribute any material that could be considered offensive, illegal or discriminatory.

6. I will respect copyright and intellectual property rights.

7. I will ensure that all electronic communications with pupils and other adults are appropriate.

8. I will not use the school system(s) for personal use in working hours (except for occasional use during breaks/lunchtimes.)

9. I will not install any hardware or software without the prior permission of the Computing Subject Leader.

10. I will ensure that personal data (including data held on SIM systems) is kept secure at all times and is used appropriately in accordance with Data Protection legislation and GDPR (2018)

11. I will abide by the school's safeguarding rules for using personal mobile equipment, including my mobile phone and other personal devices such as smart watches, at all times.

12. I will ensure that Images of pupils and/or adults will be taken, stored and used for professional purposes in line with school policy using school devices only and with written consent of the parent/carer or relevant adult. I will not distribute images outside the school network without the prior permission of the parent/carer, or person/s in the image.

13. I will report any known misuses of technology, including the unacceptable behaviours of others.

14. I have a duty to respect the technical safeguards which are in place. I understand that attempting to breach technical safeguards or gain unauthorised access to systems and services is unacceptable.

15. I have a duty to report failings in technical safeguards which may become apparent when using the systems and services.

16. I have a duty to protect passwords and personal network logins, and should log off the network when leaving workstations unattended. I understand that any attempts to access, corrupt or destroy other users' data, or compromise the privacy of others in any way, using any technology, is unacceptable.

17. I understand that network activities and online communications may be monitored, including any personal and private communications made using school systems.

18. I am aware that in certain circumstances where unacceptable use is suspected, enhanced monitoring and procedures may come into action.

19. I will take responsibility for reading and upholding the standards laid out in the AUP. I will support and promote the school's Online Safety Policy and help pupils to be safe and responsible in their use of ICT and related technologies.

20. I understand that these rules are designed for the safety of all users and that if they are not followed, school sanctions will be applied and disciplinary action taken.

21. I will undertake Prevent training provided by the school and understand that I have the duty to report any online activities that could be linked to terrorist activity or radicalisation.

---

22. Acceptable Use Policy Agreement AI:

I understand that I must use AI and emerging technologies responsibly to minimise the risk to the safety, privacy, or security of the school community and its systems. I acknowledge the potential of these technologies for enhancing learning and will endeavour to integrate them in a way that aligns with the school's policy, ethos and values.

For my professional and personal safety:

•I understand that the school will monitor my use of AI tools and technologies.

•I will only use AI tools and technologies for purposes authorised by the school and will ensure compliance with data protection laws (e.g. UK GDPR) when handling personal data.

•I will ensure that any sensitive or personally identifiable information about staff, students, or parents/carers is only entered into AI systems that have explicit approval and robust security measures in place.

•I will report any AI-related incidents or anomalies that could indicate misuse, bias, or harm to the appropriate person immediately.

In my communications and actions:

•I will respect copyright, intellectual property, and ethical standards when uploading content to prompt AI output.

•I will critically evaluate the outputs of AI systems to avoid spreading misinformation or biased content and will ensure that all AI-assisted decisions are made with appropriate human oversight.

•I will communicate professionally and responsibly when using AI systems.

•I will ensure transparency through appropriate attribution where AI has been used.

When engaging with learners:

•I will support learners on the safe, ethical, appropriate and effective use of AI.

•I will use AI tools to engage with learners in ways that uphold and enhance their privacy, wellbeing, and trust.

When using the school's systems and resources:

•I will use AI systems in compliance with established security measures and access protocols.

•I will ensure that any AI applications used in teaching or administration are vetted and comply with the school's policies.

•I will ensure generative AI tools are not used to impersonate others or create deceptive or harmful content.

When handling data:

•I will ensure compliance with the school's data protection policies when using AI for data analysis or reporting.

•I will ensure I have explicit authorisation when uploading sensitive school-related information into generative AI systems.

Responsibility and Accountability:

•I will use generative AI tools responsibly to create authentic and beneficial content, ensuring respect for individuals' identities and well-being.

•I understand that misuse of AI or emerging technologies could lead to disciplinary actions, including warnings, suspension, or referral to the appropriate authorities.

•I acknowledge that this agreement applies to all AI-related activities within and outside of school premises that are connected to my professional responsibilities.

I have read and agree to follow this code of conduct and to support the safe use of ICT throughout the school.

Signature _____ Date _____

Full Name _____
(PRINT)

Position/Role _____

Appendix 3-

ICT Acceptable Use Policy (AUP) Supply teachers and Visitors/Guests Agreement

(For use with any adult working in the school, for a short period of time.)

1. I will take responsibility for my own use of any technologies, making sure that I use them safely, responsibly and legally.

2. I will not browse, download/upload or distribute any material that could be considered offensive, illegal or discriminatory.
3. I will not use any external device to access the school's network e.g. pen drive.
4. I will respect copyright and intellectual property rights.
5. I will ensure that images of pupils and/or adults will be taken, stored and used for professional purposes in line with school policy and with written consent of the parent/carer or relevant adult. I will not distribute images outside the school network without the prior permission of the parent/carer, or person/s in the image.
6. I understand that network activities and online communications are monitored, including any personal and private communications made using school systems.
7. I will not install any hardware or software onto any school system.
8. I understand that these rules are designed for the safety of all users and that if they are not followed, school sanctions will be applied and disciplinary action taken.
9. I understand that the use of personal mobile phones is not permitted in classrooms or any other room where children may be present.
10. I understand that personal mobile technology will not be used to take photographs within school.

Acceptable Use Policy Agreement AI:

I understand that I must use AI and emerging technologies responsibly to minimise the risk to the safety, privacy, or security of the school community and its systems. I acknowledge the potential of these technologies for enhancing learning and will endeavour to integrate them in a way that aligns with the school's policy, ethos and values.

For my professional and personal safety:

•I understand that the school will monitor my use of AI tools and technologies.

•I will only use AI tools and technologies for purposes authorised by the school and will ensure compliance with data protection laws (e.g. UK GDPR) when handling personal data.

•I will ensure that any sensitive or personally identifiable information is only entered into AI systems that have explicit approval and robust security measures in place.

•I will report any AI-related incidents or anomalies that could indicate misuse, bias, or harm to the appropriate person immediately.

In my communications and actions:

•I will respect copyright, intellectual property, and ethical standards when uploading content to prompt AI output.

•I will critically evaluate the outputs of AI systems to avoid spreading misinformation or biased content and will ensure that all AI-assisted decisions are made with appropriate human oversight.

•I will communicate professionally and responsibly when using AI systems.

•I will ensure transparency through appropriate attribution where AI has been used.

When engaging with learners:

•I will support learners on the safe, ethical, appropriate and effective use of AI.

•I will use AI tools to engage with learners in ways that uphold and enhance their privacy, wellbeing, and trust.

When using the school's systems and resources:

•I will use AI systems in compliance with established security measures and access protocols.

•I will ensure that any AI applications used in teaching or administration are vetted and comply with the school's policies.

•I will ensure generative AI tools are not used to impersonate others or create deceptive or harmful content.

When handling data:

•I will ensure compliance with the school's data protection policies when using AI for data analysis or reporting.

•I will ensure I have explicit authorisation when uploading sensitive school-related information into generative AI systems.

Responsibility and Accountability:

•I will use generative AI tools responsibly to create authentic and beneficial content, ensuring respect for individuals' identities and well-being.

•I understand that misuse of AI or emerging technologies could lead to disciplinary actions, including warnings, suspension, or referral to the appropriate authorities.

•I acknowledge that this agreement applies to all AI-related activities within and outside of school premises that are connected to my professional responsibilities.

I have read and agree to follow this code of conduct and to support the safe use of ICT throughout the school.

Signature_____
Date_____

Full Name _____ (PRINT)

Position/Role _____

Appendix 4

ICT Acceptable Use Policy (AUP) Children- KS2

These rules reflect the content of our school's Online Safety Policy. It is important that parents/carers read and discuss the following statements with their child(ren), understanding and agreeing to follow the school rules on using ICT, including use of the Internet.

1. I will only use ICT (e.g. computers, i-Pads etc) in school for school purposes.
2. I will not bring equipment such as mobile phone, mobile games consoles or tablets into school unless specifically asked/pre agreed by my teacher.
3. I will only use the Internet and/or online tools when directed by a member of staff.
4. I will only use my class e-mail address in school when emailing
5. I will not deliberately look for, save or send anything that could be unpleasant, nasty or embarrassing to anyone including me.
6. I will not deliberately bring in inappropriate electronic materials from home e.g video clips/films that aren't appropriate for my age.
7. I will not deliberately look for, or access inappropriate websites.
8. If I accidentally find anything inappropriate or feel uncomfortable, I will tell my teacher immediately.
9. I will only communicate online with people a trusted adult has approved.
10. I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.
11. I will not give out my own, or others', details such as names, phone numbers or home addresses.
12. I will not tell other people my ICT passwords except a trusted adult.
13. I will not arrange to meet anyone that I have met online.
14. I will only open/delete my own files at my teacher's request.
15. I will not attempt to download or install anything on to the school network without permission.
16. I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
17. I know that my use of ICT can be checked and that my parent/carer contacted if a member of school staff is concerned about my online safety.
18. I understand that if I don't follow the rules that the school may take disciplinary steps in line with the school's Behaviour Policy. This could mean being given a warning or even banned from using certain ICT equipment for a while if I did something very serious.

Appendix 5

ICT Acceptable Use Policy (AUP) Children- KS1 & EYFS

These rules reflect the content of our school's Online Safety Policy. It is important that parents/carers read and discuss the following statements with their child(ren), understanding and agreeing to follow the school rules on using ICT, including use of the Internet.

1. I will look after the ICT equipment that I use such as computers, iPads or cameras.

2. I will only use activities that a teacher or suitable adult has told or allowed me to use

3. I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong

4. I will tell a teacher or suitable adult if I see something that upsets me on the screen

5. I will not tell anyone about myself online (this is my name, home or school address, school name etc).

6. I will not upload pictures or digital images of myself or others.

7. I will only send polite messages

8. I know that if I break the rules I might not be allowed to use a computer or iPad.

Appendix 6

Online Safety Rules (Displayed in every classroom)

Designated Safeguarding Lead (DSL) notified of an Online Safety incident[1]

Carry out immediate safeguarding actions necessary to protect individuals

Unsuitable or inappropriate materials or activity

Illegal materials or activities found/suspected

Convene Safeguarding Incident Review Meeting

Investigate incident and discuss with the learner / staff / to determine what happened

Update parents/carers on incident as applicable

Ensure the wellbeing of those involved is addressed.

Ensure Incident Log is updated and make available as required

Review policies & processes and identify learning opportunities

Ensure updates to practice are shared with staff

Implement changes and monitor situation.

Wellbeing of a child potentially at risk

Staff, volunteer or another adult

Follow established safeguarding arrangements and report to the Police immediately

Refer to the LA, LADO and follow HR processes

Secure and preserve evidence in-line with Police/DOS/Safeguarding advice. Remember, do NOT investigate yourself.

Await Police response

If no illegal activity or content is confirmed, revert to internal procedures

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

In the case of a member of staff or volunteer, it is possible that a suspension will take place at the point of referral to the Police whilst investigations are undertaken. Always ensure DOS advice and HR processes are correctly applied and followed

[1] This flowchart provides a suggested outline process for dealing with online safety incidents. You may wish to adapt and align with existing safeguarding policy and practice to ensure there is a consistent approach to managing safeguarding incidents in your setting.
[2] The Incident Review Meeting (IRM) will typically take place as soon as possible after a serious incident to determine next steps and will usually follow any immediate safeguarding actions that have been taken (note: less serious incidents may not require an IRM).

Appendix 8: Policy on the use of Artificial Intelligence in Schools

Statement of intent

Artificial Intelligence (AI) technology is already widely used in commercial environments and is gaining greater use in education. We recognise that the technology has many benefits and the potential to enhance outcomes and educational experiences, with the opportunity to support staff in reducing workload.

We also realise that there are risks involved in the use of AI systems, but that these can be mitigated through our existing policies and procedures, amending these as necessary to address AI risks.

We will educate staff and learners about safe and ethical use of AI, preparing them for a future in which AI technologies are likely to play an increasing role.

The safeguarding of staff and learners will, as always, be at the forefront of our policy and practice.

Policy Statements

- The school acknowledges the benefits of the use of AI in an educational context - including enhancing teaching and learning and outcomes, improving administrative processes, reducing workload and preparing staff and learners for a future in which AI technology will be an integral part. Staff are encouraged to use AI based tools to support their work where appropriate, within the frameworks provided below and are required to be professionally responsible and accountable for this area of their work.
- We will comply with all relevant legislation and guidance, with reference to guidance contained in Keeping Learners Safe
- We will provide relevant training for staff and governors in the advantages, use of and potential risks of AI. We will support staff in identifying training and development needs to enable relevant opportunities.
- We will ensure that, within our education programmes, learners understand the ethics and use of AI and the potential benefits and risks of its use. The school recognises the importance of equipping learners with the knowledge, skills and strategies to engage responsibly with AI tools.
- As set out in acceptable use agreements, the school will use AI responsibly and with awareness of data sensitivity. Where used, staff should use AI tools responsibly, ensuring the protection of both personal and sensitive data. Staff should only input anonymized data to avoid the exposure of personally identifiable or sensitive information.
- Staff should always ensure AI tools used comply with UK GDPR and other data protection regulations. They must verify that tools meet data security standards before using them for work related to the school.
- Only those AI technologies approved by the school may be used. Staff should always use school-provided AI accounts for work purposes. These accounts are configured to comply with organisational security and oversight requirements, reducing the risk of data breaches.
- We will protect sensitive information. Staff must not input sensitive information, such as internal documents or strategic plans, into third-party AI tools unless explicitly vetted for that purpose. They must always recognize and safeguard sensitive data.
- The school will ensure that when AI is used, it will not infringe copyright or intellectual property conventions – care will be taken to avoid intellectual property, including that of the learners, being used to train generative AI models without appropriate consent.
- AI incidents must be reported promptly. Staff must report any incidents involving AI misuse, data breaches, or inappropriate outputs immediately to the relevant internal teams. Quick reporting helps mitigate risks and facilitates a prompt response.
- The school will audit all AI systems in use and assess their potential impact on staff, learners and the school's systems and procedures, creating an AI inventory listing all tools in use, their purpose and potential risks.

- We are aware of the potential risk for discrimination and bias in the outputs from AI tools and have in place interventions and protocols to deal with any issues that may arise. When procuring and implementing AI systems, we will follow due care and diligence to prioritise fairness and safety.
- The school will support parents and carers in their understanding of the use of AI in the school
- AI tools may be used to assist teachers in the assessment of learner's work and identify areas for improvement. Teachers may also support learners to gain feedback on their own work using AI. Use of these tools should be purposeful, considered and with a clear focus on ensuring impact and understanding and mitigating risk
- Maintain Transparency in AI-Generated Content. Staff should ensure that documents, emails, presentations, and other outputs influenced by AI include clear labels or notes indicating AI assistance. Clearly marking AI-generated content helps build trust and ensures that others are informed when AI has been used in communications or documents.
- We will prioritise human oversight. AI should assist, not replace, human decision-making. Staff must ensure that final judgments, particularly those affecting people, are made by humans and critically evaluate AI-generated outputs. They must ensure that all AI-generated content is fact-checked and reviewed for accuracy before sharing or publishing. This is especially important for external communication to avoid spreading misinformation.
- Recourse for improper use and disciplinary procedures. Improper use of AI tools, including breaches of data protection standards, misuse of sensitive information, or failure to adhere to this agreement, will be subject to disciplinary action as defined in Staff Disciplinary Policy.

Responsibilities

Headteacher and Senior Leaders

Are responsible for the strategic planning of how AI will be used in the school, establishing AI policies and procedures and ensuring that all staff receive relevant training and have a clear understanding of these.

Designated Safeguarding Person (DSP) / Online Safety Lead

Our Designated Safeguarding Person / Online Safety Lead has responsibility for online safety in the school. They are expected to have knowledge of AI and its safeguarding implications and an in-depth working knowledge of key guidance. We ensure that they receive appropriate specialist training, commensurate with their role and that ongoing training is provided for all school staff.

Data Protection Officer

The DPO will be responsible for providing advice and guidance about data protection obligations in relation to the use of AI, including related Data Protection Impact Assessments (DPIAs).

Technical Staff

Technical staff / IT Leads will be responsible for technical support and guidance, with particular regard to cyber-security and the effectiveness of filtering and monitoring systems. (

Staff

It is the responsibility of all staff to have read and understood this policy and associated Acceptable Use Agreements. All staff must report any incidents or suspected incidents concerning the use of AI in line with school policy. All staff will challenge any inappropriate behaviour. Staff have a duty to ensure that:

- the school environment is safe
- sensitive and confidential data / information is secure
- that their actions do not put the reputation of the school at risk and that
- learners understand their responsibilities

Governors

We ensure that our governing body has a good understanding of how AI is used in a school context and potential benefits and risks of its use. They receive regular training and updates, enabling them to support the school and challenge where necessary. This may include evaluation of the use of AI in the curriculum, administration and communications, ensuring that risks relating to these issues are identified, that reporting routes are available, and that risks are effectively mitigated.

Parents/carers

We work hard to engage parents and carers by:

- *sharing newsletters*
- *sharing information online e.g., website, social media*
- *providing curriculum information*

Our parents and carers are made aware of how AI is used in school and receive guidance on both good practice in its use and the risks of misuse that may affect their childrens' learning or safety. They are encouraged to report any concerns to the school and are made aware that all incidents will be handled with care and sensitivity.

Vulnerable groups

We recognise that vulnerable learners are more likely to be at risk from the misuse of AI (both in their own use or through the actions of others). We ensure that vulnerable learners are offered appropriate support to allow them to gain full benefit of the use of AI, while being aware of the potential risks.

Children are considered to be vulnerable data subjects and therefore any process involving their personal data is likely to be "high risk". If an AI/ automated process is used to make significant decisions about people, this is likely to trigger the need for a Data Protection Impact Assessment (DPIA).

Reporting

Our reporting systems are well promoted, easily understood and easily accessible for staff, learners and parents/carers to confidently report issues and concerns, knowing these will be treated seriously. All reports will be dealt with swiftly and sensitively and outcomes shared where appropriate. We also respond to anonymous reports, or reports made by third parties. This can be done via:

- nominated member of staff

- established school reporting mechanisms (CPOMS)
- online/offline reporting tool
- anonymous/confidential reporting routes online

Responding to an incident or disclosure

Our response is always based on sound safeguarding principles and follows school safeguarding and disciplinary processes. It is calm, considered and appropriate and puts the learner at the centre of all decisions made.

- All AI incidents (including data breaches and/or inappropriate outputs) must be reported promptly to the relevant internal teams. Effective reporting helps mitigate risks and facilitates a prompt response.
- Where relevant / required incidents will be reported to external agencies e.g., Police, LADO
- All AI related incidents will be recorded through the school's normal recording systems

In the case of misuse of AI by staff, the normal staff disciplinary processes will be followed.

Risk assessment

It is key that our approach to managing risk aligns with, and complements, our broader safeguarding approach.

The school understands that despite many positive benefits in the use of AI, there are some risks that will need to be identified and managed, including:

- Legal, commercial, security and ethical risks
- Data Protection
- Cyber Security
- Fraud
- Safeguarding and well-being
- Duty of care

Our school's educational approach seeks to develop knowledge and understanding of emerging digital technologies, including AI.

This policy outlines our commitment to integrating Artificial Intelligence (AI) responsibly and effectively within our school environment. We will use AI responsibly, safely and purposefully to support these aims:

- Enhance academic outcomes: Improve educational experiences and performance for pupils.
- Support teachers: Assist in managing workloads more efficiently and effectively.
- Educate on AI use: Promote safe, responsible, and ethical AI practices among staff and learners.
- Develop AI literacy: Incorporate AI as a teaching tool to build AI skills and understanding.
- Prepare for the future: Equip staff and pupils for a future where AI is integral.

- Promote educational equity: Use AI to address learning gaps and provide personalised support.

Our school's approach is to deliver this knowledge and understanding wherever it is relevant within the curriculum. This will include:

- Computing
- PHSE
- Cross curricular programmes
- Assemblies

Our approach is given the time it deserves and is authentic i.e., based on current issues nationally, locally and within our school's risk profile. It is shaped and evaluated by learners and other members of the school community to ensure that it is dynamic, evolving and based on need. We do this through:

- *Learner assessment*
- *Critical evaluation of emerging trends and research findings*
- *Parental engagement*
- *Staff consultation*
- *Engaging with learners*
- *Staff training*

Training

As AI becomes an integral part of modern education, it is essential for staff to be trained in its effective use. Training equips educators with the knowledge and skills to integrate AI tools responsibly into teaching, learning, and administrative processes. It ensures that AI is used to enhance educational outcomes, streamline workloads, and promote equity while safeguarding ethical practices and data privacy. By fostering AI literacy, staff can confidently prepare pupils for a future where AI is a key driver of innovation and opportunity.

- We will provide training to all staff on the effective, responsible, and ethical use of AI technologies in education, ensuring these tools enhance teaching, learning, and administrative processes.
- We will integrate AI-related risks and safeguards into annual safeguarding training, aligning with statutory guidance, including "Keeping Learners Safe."
- We will ensure all staff are equipped with the knowledge and skills to confidently integrate AI into their professional practice and to prepare pupils for a future shaped by AI-driven innovation and opportunities.
- We will train staff to identify, assess, and mitigate risks associated with AI technologies, including issues such as biased algorithms, privacy breaches, and harmful content.
- We will train staff on robust data protection practices, ensuring compliance with UK GDPR and other relevant regulations while using AI systems.
- We will promote ethical practices in the use of AI, ensuring that these technologies contribute to equity, fairness, and inclusivity in education.
- We will empower educators to teach learners about the safe and ethical use of AI, cultivating a culture of awareness, resilience, and informed decision-making in the digital age.
- We will train staff to use AI responsibly as a tool to monitor and address online risks, reinforcing our commitment to a safe learning environment.