Inspire Learning, Ignite Curiosity

Marlow C of E Infant School
Online Safety Policy
2025

Then God said, "Let us make humankind in our image, in our likeness"
Genesis 1:26

Rationale

At Marlow Church of England Infant School our curriculum vision is to inspire learning and ignite curiosity within a welcoming Christian and spiritual community. We embrace the uniqueness of everybody and are inclusive of all. Our values of respect, kindness, perseverance, forgiveness, thankfulness and service guide all that we do and our aim is for every child to feel nurtured, supported and safe.

Our belief is that every individual is created in God's image and therefore is precious and valuable. We believe in treating everybody with respect and dignity because we acknowledge everyone's God given value and unique identity

We aim to achieve this by providing children with the opportunity to work towards achieving their full potential by:

- Embracing the uniqueness of everybody and be inclusive of all
- Empowering all to be enthusiastic learners
- Ensuring that every child feels nurtured, supported and safe
- Enriching learning through progressive teaching methods and technology
- Being responsible to and for society
- Being good citizens of the planet

As a school we support the rights of children and these rights are encompassed in UN Convention of the Rights of the Child. This policy focuses on helping to realise Article 19*: You have the right to be protected from being hurt and mistreated, in body or mind* and Article 28: *You have the right to a good quality education.*

At Marlow C of E Infant School, we consider that Online Safety should be approached at a whole school level and forms part of our statutory safeguarding responsibilities.

Aims

Through this policy we aim:

- To ensure the safety of pupils and staff whilst they use technology to enhance, receive/deliver a high-quality education.
- Establish the ground rules that are in place at Marlow C of E Infant School for using the internet and digital communications such as mobile phones, collaboration tools and personal publishing. It highlights the need to educate the pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.
- Describe how these fit into the wider context of other school policies.
- Demonstrate the methods used to protect children from accessing sites containing inappropriate material such as pornography, racist or politically extreme views and violence.

Scope

This policy applies to all members of the school community (including staff, students / pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school IT systems, both in and out of the school.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of students 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 radicalisation, cyber-bullying, or other online safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data.

Introduction

At Marlow Infant School we value the use of new technologies for both teaching and learning. We recognise that digital communication, website use and mobile technologies have become integral to the lives of our pupils, both within schools and in their lives outside school. New technologies will continue to be relevant to our pupils in their futures, for continuing education, employment and recreation.

Children at Marlow Church of England Infant School have an entitlement to safe internet access, which is part of the school's wider duty of care. With the support of TurnITon, we take steps to limit the risks associated with internet use, whilst recognising that it is impossible to eliminate all risks. We acknowledge that many of the risks associated with internet use mirror those which exist in the offline world. For this reason, we educate children to be aware of the dangers of internet use, to know how to avoid them and when to ask for help.

We recognise that as a school we have a responsibility in educating parents about the dangers as well as the benefits of internet use. Parents are encouraged to supervise internet use and be aware of their children's online behaviour in order to promote safe use.

Online Safety encompasses the use of new technologies, internet and digital communications such as mobile phones, collaboration tools and personal publishing.

The school's Online Safety policy will operate in conjunction with other policies:

- Behaviour
- Anti-bullying
- Child Protection
- Curriculum (specifically the Computing and PSHE/RSE curricula)
- Data Protection
- Mobile Technology
- Use of images

Online safety relies on effective practice at a number of levels:

- Responsible IT use by all staff and students encouraged by education and made explicit through published policies
- Sound implementation of online safety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband including the effective management of filtering
- The support of the Headteacher and Governing Body

Roles & Responsibilities

Designated Safeguarding Lead

'The DSL continues to have overall responsibility for online safety; they can be supported by appropriately trained deputies and should liaise with other staff as appropriate, but this responsibility cannot be delegated'. KCSIE

The Designated Safeguarding Leads ensure that they are trained in online safety issues appropriate training to ensure they understand the unique risks associated with online safety, can recognise the additional risks learners with SEN and disabilities (SEND) face online, and have the relevant knowledge and up to date capability required to keep children safe online.

The areas that this capability covers (but not limited to):

- sharing of personal data
- access to illegal/inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying
- anti-terrorism and radicalisation

There are four main areas of a DSLs responsibilities with regards to Online Safety:

1. ***Policies and procedures***

- Main point of contact for online safety issues
- Ensuring that there are robust policies and procedures are in place and implemented
- Maintaining reporting channels and signposting to support
- Recording online safety incidents and actions
- Ensuring that the whole school community understands what is appropriate online behaviour and understands the sanctions for misuse.
- Liaising with the local authority and other bodies as appropriate

2. ***Infrastructure and Technology***

- Ensuring that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- Providing training and advice for staff
- Liaising with IT support company – TurnITon- and the Senior Leadership Team to implement filter and monitoring systems
- Regularly reviewing the filtering and monitoring of the IT systems
- Acting in line with child protection policies and checking whether the filtering and monitoring system identifies concerns
- Working with the Data Protection Officer and Data Protection Lead to ensure that online practices are in line with current laws
- Receiving reports of online safety incidents and creating a log of incidents to inform future online safety developments

3. ***Education and Training***

- Implementing online safety training for all staff
- Ensuring that all staff receive information and training which addresses inline safety at induction.
- Working with staff to embed online safety education throughout the curriculum
- Engaging with local and national events to promote positive online safety behaviour – eg Safer Internet Day and Anti Bullying Week
- Promoting online safety to parents and carers and the wider community
- Ensuring that knowledge and skills are refreshed at regular intervals

4. ***Standards and inspections***

- Evaluating the delivery and impact of online safety policy and practice
- Reviewing reported online safety incidents
- Feeding back online safety issues to Senior Leaders and other agencies where appropriate.

Governors
Governing bodies should ensure that, as part of the requirement for staff to undergo regular updated safeguarding training, including online safety and the requirement to ensure children are taught about safeguarding, including online safety, that safeguarding training for staff, including online safety training, is integrated, aligned and considered as part of the whole school or college safeguarding approach and wider staff training and curriculum planning.

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 Governors receiving regular information about online safety incidents and monitoring reports. The Safeguarding Governor has taken on the role of Online Safety Governor. This aspect of the Safeguarding Governor's role will include:

- liaison with the Designated Safeguarding Lead
- regular monitoring of online safety incident logs
- regular monitoring of filtering/change control logs
- reporting to relevant Governors/Board/Committee/meeting

Network Manager
Marlow C of E Infant School has a managed ICT service provided by TurnITon and it is the responsibility of the school to ensure that they carry out all the required online safety measures. The Headteacher/Designated Safeguarding Lead ensures that TurnITon are aware of the School's Online Safety policy and procedures.
.
The Network Manager at Marlow C of E Infant School is the Headteacher who is responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets required online safety technical requirements and any Local Authority that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are changed periodically
- 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 effectively carry out their online safety role and to inform and update others as relevant
- attempted misuse to be reported to the Designated Safeguarding Lead/Headteacher for investigation.

All Staff

- All staff should be aware that technology is a significant component in many safeguarding and wellbeing issues.
- Children are at risk of abuse online as well as face to face. In many cases abuse will take place concurrently via online channels and in daily life.
- Children can also abuse their peers online, this can take the form of abusive, harassing, and misogynistic messages, the non-consensual sharing of indecent images, especially around chat groups, and the sharing of abusive images and pornography, to those who do not want to receive such content.

All staff should ensure 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 (AUP)
- they report any suspected misuse or problem to the Designated Safeguarding Leads for investigation
- all digital communications with students / parents / carers should be on a professional level and only carried out using official school systems
- online safety is embedded in all aspects of the curriculum
- pupils understand and follow the online safety rules
- they monitor the use of digital technologies, mobile devices, cameras, etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- in lessons processes are in place for dealing with any unsuitable material that is found in internet searches

Pupils

Pupil will be taught at an age appropriate level:

- About their responsibility to use technology sensibly and safely
- To understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- The importance of adopting good online safety practice when using digital technologies in and out of school.

Parents / Carers

Parents/Carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' workshops, newsletters, surveys and website information about online safety campaigns. Parents and carers will be encouraged to support the school in promoting good online safety practice and ensure the appropriate use of digital and video images taken at school events and undertaking that these are taken for private use only

Use of IT Equipment

Children are taught to treat the hardware with respect and to follow behaviour routines and safe usage procedures.

- When children log on to the network they have to agree to a safe usage policy on every occasion. This is explained and discussed at the start of every year and repeated when an incident or misunderstanding has occurred.
- The school ensures that users may only access the school's networks through a password and personal log-in. Children are given a password which is available to the teacher, and teachers can use their own log-in to access all pupil files.
- Staff are able to change their own passwords. Children are taught the importance of password security.
- Parents are asked to sign an acceptable use policy and to share the requirements with their children.
- Safer Internet Day (SID) is observed annually in school. There is an assembly and suggested materials for use in class. Older children make posters about safe internet use and cyber-bullying which are displayed around school.
- Tips for safe internet use at home are shared with parents at least once each year, to coincide with SID and in response to any reported issues with internet usage in school or at home. These are shared through the school newsletter and separate booklets. We provide a range of information to support parents with Online safety on the school website.

Teaching and Learning

The internet is an essential element in 21st century life for business and social interaction. The school has a duty to provide children and staff with quality internet access as part of the learning experience. Internet access is part of the statutory curriculum and a necessary tool for students and staff.

Internet Access

Internet access is filtered for all users. Differentiated internet access is available for staff and customised filtering changes are managed by TurnITon on behalf of the School. Filtered access is via the Internet Service Provider, Exa using SSL certificates.

There is a clear route for reporting and managing changes to the filtering system. Where personal mobile devices are allowed internet access through the school network, filtering will be applied that is consistent with school practice.

- In the event of the technical staff needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Headteacher
- Mobile devices that access the school internet connection (whether school or personal devices) will be subject to the same filtering standards as other devices on the school systems
- Any filtering issues should be reported immediately to the filtering provider via TurnITon.
- Requests from staff for sites to be removed from the filtered list will be considered by the Headteacher/Designated Safeguarding Lead. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the Safeguarding Governor

Education / Training / Awareness

Pupils will be made aware of the importance of filtering systems through the online safety education programme. They will also be warned of the consequences of attempting to subvert the filtering system.

Pupils are taught about acceptable internet use and are given clear objectives for internet use. Pupils and staff are expected to acknowledge and agree to the acceptable use policy when logging onto the curriculum system with their individual passwords.

Pupils are taught about effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation

Pupils are taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy

Staff users will be made aware of the filtering systems through:

- the Acceptable Use Agreement
- induction training
- staff meetings, briefings, INSET

Staff are not permitted to access the school's wireless technology with their personal laptops unless they have Sophos – anti virus software installed on their laptops

Staff using school laptops at home are aware that Exa filtering is installed on all units and that the appropriate use of the equipment will be monitored when the laptop accesses the school's wireless system on its return to school.

Parents will be informed of the school's filtering policy through the Acceptable Use Agreement and through online safety awareness sessions / newsletter etc.

The school ensures that the use of the internet derived materials by staff and pupils complies with copyright law.

E-Mail
Pupils may only use approved e-mail accounts on the school system where available.

Pupils must immediately tell a teacher if they receive offensive material or comments via e-mail. Pupils must not reveal personal details of themselves or others in electronic communication, or arrange to meet anyone.

E-Mails sent to an external organisation must be authorised before sending, in the same way as a letter written on school headed paper. Staff should not give out personal e-mail addresses.

School Website
The School's contact details are on the school website. The school address, e-mail and telephone number are all available there.

Staff and pupil details or personal information is not published.

The Headteacher has overall editorial responsibility and ensures that the content of the school website is accurate and appropriate.

Photographs that include pupils are selected carefully so that they do not include children whose parents have not given permission for the use of their child's image on the website.

Written permission from parents/carers is obtained before photographs of pupils are published on the website.

Pupil's full names are not used anywhere on the website.

Mobile Technology
In order to ensure the safety of both children and staff, mobile phones are not allowed in the vicinity of children during the school day

Staff mobile phones should be turned off /left on silent and locked in the classroom cupboard, staff room or school office at all times during teaching sessions. Under no circumstances should they be used/visible when in the classrooms or areas that the children use. If it is felt necessary to make phone calls/take messages during the school day this must occur during lunch / break times in an area where there are no children (e.g. the staff room). (Smart watches should have their Bluetooth connection turned off when in the same areas as per the terms of Mobile phone use above)

Staff should use the school mobile phone when off site on school trips. Staff should not give out personal mobile numbers to pupils or parents.

Pupils are not permitted to bring mobile phones and other devices with photographic / video capability into school except with the express permission of the Headteacher / senior staff.

Staff should refer to the school's Mobile Technology Policy on the use of mobile devices in school.

Digital Images and Video

At Marlow C of E Infant School, we value the use of photographs in our school displays; on our walls, in children's workbooks, and on our website.

Parents are asked annually if they wish to give their permission for photographs to be used in school, on the website or in advertising/publicity materials. (Parents can agree to some, all or none of the above as they see fit).

Staff may only use school's equipment to take pupil photographs during lessons and other activities including school outings. These photographs must only be uploaded to the school's network.

Children are encouraged to take photographs themselves, and to be aware of taking a decent image which others are happy with.

Parents and volunteers who accompany outings or attend school events such as assemblies, plays or sports days are asked not to take or distribute photographs without permission of the parents of the children in them.

Parents are also reminded on every such occasion that they must not share photographs or videos on social media sites.

Photographs/videos taken during school trips should only be taken by staff members on school devices which are directly downloaded into the appropriate folder on the school network.

If pupils use the school devices, the teacher responsible for the group should supervise the shot where possible.

Parent volunteers on trips are instructed that they are not allowed to take photographs on their mobile phones / devices.

All photographs taken by children and staff should be scrutinised by the teacher for suitability before being used for any purpose.

Photos are stored on the school network in line with the retention schedule of the school Data Protection Policy. Staff and parents are reminded annually about the importance of not sharing without permission, due to reasons of child protection, data protection, religious or cultural reasons, or simply for reasons of personal privacy

Managing Technologies

Emerging technologies are evolving at a rapid rate and although every attempt is made to protect children from offensive or inappropriate material and misuse, there may be occasions when inadvertent access occurs. The following points apply:

- If staff or pupils discover an unsuitable site, it must be reported immediately to the Headteacher/Designated Safeguarding Lead who will report the site to TurnITon to ensure that the site is blocked.
- If it is felt that the incident is a child protection issue, the procedure outlined in the 'What to do in the event of an Online Safety Incident' flow chart (*Appendix1*) for reporting this will immediately be put into place.
- All internet access including e-mails will be monitored through the Exa filtering programme. The level of filtering is determined by the login profile used. Default filtering used is a child's login profile, with high levels of filtering.
- All photographs / videos should be viewed by the teacher for appropriateness before publishing openly. Photographs which may cause the subject to be embarrassed or upset should be deleted.
- Any child taking photographs deemed to be inappropriate should be dealt with in terms of the behaviour policy.

Social Media

The school blocks access to all social networking sites for pupils. Pupils are taught never to give information which may allow them to be identified.

Marlow C of E Infant School recognises that many staff, governors, parents, carers and pupils use the internet for personal purposes and that they may participate in social networking on social media websites such as Facebook, Twitter, Youtube, etc.

In addition, staff, governors, parents and carers may set up personal weblogs or "blogs" on the internet. Whilst staff, governors, parents and carers are free to use the internet in this way, they must ensure that they do not breach the law or disclose Marlow C of E Infant School's confidential information, breach copyright, defame the school, its staff, governors, parents, carers and pupils.

They must not disclose personal data or information about any individual that could breach the General Data Protection Regulation 2018 and the other principles outlined in this Online Safety policy. They should keep completely confidential, any information regarding the children, their families or other staff which is learned through the school.

Social media technologies take on many different forms including magazines, Internet forums (message boards), blogs, microblogging (Twitter, Reddit), social media networks (Facebook, Instagram, WhatsApp, etc), podcasts, photographs or pictures, video and virtual game worlds.

Websites and Blogs

The following guidelines apply:

- Staff, governors, parents and carers must not disclose any information that is confidential to the school or any third party that has disclosed information to the school.
- Staff, governors, parents and carers should not link any personal websites, social networking sites etc to the school's website.
- Staff, governors, parents and carers must not use the school website, internet systems, e-mail addresses or intranet for their blog and staff must not write their blog in employer time.
- If a member of staff, governor, parent or carer is asked to contribute to an official blog connected to the school, then special rules will apply and they will be told in detail how to operate and what to write.
- Marlow C of E infant School will not tolerate criticisms through social media websites and blogs. If a member of staff feels aggrieved then they must follow the procedures outlined in the Complaints and Whistleblowing Policy.

Social Media Networking sites

The school respects a member of staff's right to a private life. However; the school must also ensure that confidentiality and its reputation are protected. The school expects all staff, governors, parents and carers to:

- Ensure that they do not conduct themselves in a way that is detrimental to the school.
- Take care not to allow their interaction on these websites to damage working relationships between members of staff and clients of the school.

Important Considerations
When writing a blog and placing information on social media networking sites, staff, governors, parents and carers should follow these guidelines:

- Do not include any information that breaches copyright and should link to other material rather than cutting and pasting it
- Do not defame (libel) anyone. A member of staff, governor, parent or carer who makes a defamatory statement that is published on the internet may be legally liable for any damage to the reputation of the individual concerned
- Include personal information about an individual without his/her consent, otherwise they risk breaching the General Data Protection Regulation 2018 which is a criminal offence
- Include material that is abusive, defamatory, sexist, racist or that could be interpreted as harassment or bullying
- Bring Marlow C of E Infant School into disrepute
- Staff should only access social media sites in their own time
- Staff should not comment on any posts made by others relating to the school
- Staff should not share or discuss matters relating to the school
- It is not advisable to invite parents/carers to become your friends on social networking sites. There may be a conflict of interest and security and privacy issues, but where relationships are already established, staff should proceed with caution, being fully aware of the social media guidelines and the teacher's code of conduct
- Staff should not accept friend requests from Marlow C of E Infant School pupils under any circumstances
- Staff should use the privacy settings available
- Staff should not share personal conversations.
- Staff should behave respectfully and should not engage in topics that may be considered objectionable or inflammatory

Cyber bullying
Marlow C of E Infant School is committed to ensuring that all of its staff, parents/carers and pupils are treated with dignity and respect. Bullying and harassment of any kind will not be tolerated. Cyber-bullying methods could include text messages, emails, phone calls, instant messenger services, circulating photos or video clips or by posting comments on web sites, blogs or in chat rooms or social media. Personal blogs or social media entries that refer to colleagues without their consent is also unacceptable. Staff, governors, parents and carers who cyber-bully could also face criminal prosecution under various laws, including the Malicious Communications Act 1988.

Online safety Curriculum
Online safety teaching at Marlow Infant School includes the following at age appropriate levels:

- Awareness about the need to avoid sharing of personal information including sending compromising images
- Awareness of being subject to grooming by those with whom they make contact on the internet
- Encouragement to make online friends only with people they know in the offline world
- Knowledge of how to deal with Cyber-bullying
- Understanding that they could be involved in Cyber-bullying as a victim or perpetrator
- Understanding that downloading could involve illegal activity or be damaging to the hardware, and encouraging children to ask for help
- Awareness that excessive screen-time use could lead to physical, social or emotional damage to the child

Policy Decisions
All staff, pupils and parents must agree to the IT acceptable use policy, (AUP).
*(**See Appendices II-VI**)*

- The AUP is regularly explained to the children at their level to ensure their understanding.
- The AUP is included in the home / school agreement to ensure that parents are aware of the high priority that the school places on the safe use of technologies.
- The school keeps a record of all staff and pupils who are granted internet access.
- Access to the internet will be by adult demonstration with directly supervised access to approved online sites.

Assessing Risks

The school takes all reasonable precautions to ensure that users access only appropriate material through the use of filtering programmes. Supervised access is always recommended as the school is aware that no firewall system is completely infallible.
The school audits IT provision on an annual basis to establish if the Online safety Policy is adequate and that its implementation is effective.

Handling Online Safety complaints

The Designated Safeguarding Lead is responsible for regularly monitoring internet use and updates the Headteacher and Governors on a termly basis.

The Designated Safeguarding Lead will inform class teachers if it is felt that there has been an infringement of the AUP by a child in the class. Minor infringements will first result in a warning given to the child. Further or more serious infringements will be dealt with under the school's behaviour policy.

Any infringement of the school policy by pupils or staff which is deemed to be a child protection issue will immediately be reported to the appropriate authorities the procedures outlined in the Appendix 1 – 'What to do in the event of an Online Safety Incident' Flow Chart

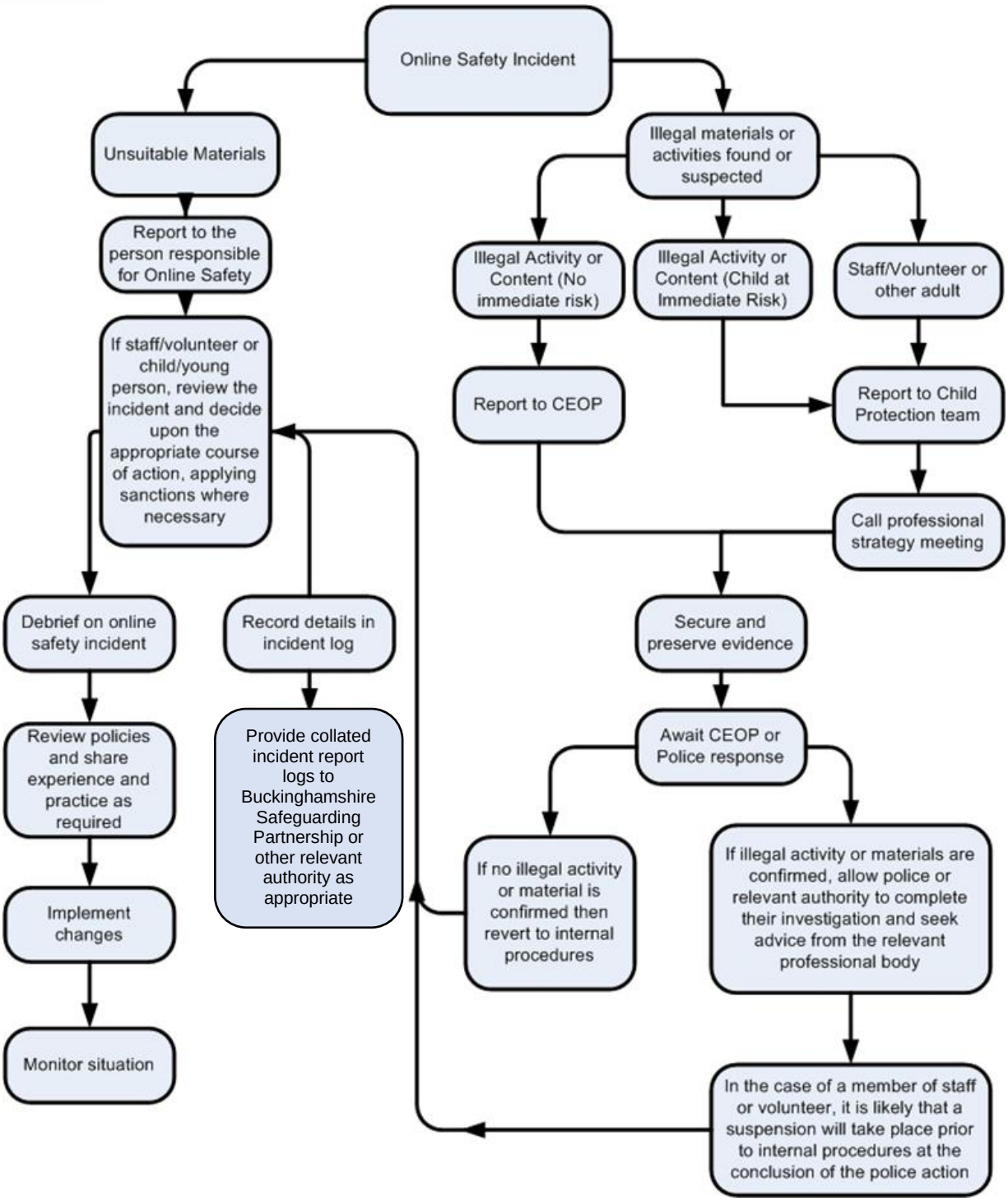
Incidents where staff are suspected of having obscene images on a mobile device will be dealt with according to the School's Disciplinary Policy.

Policy Date: January 2025

Policy Review: January 2028

Appendix I

What to do in the event of an Online Safety Incident



Appendix II

Inspire Learning, Ignite Curiosity

Marlow C of E Infant School
Acceptable Use Policy & Agreement
2025

Then God said, "Let us make humankind in our image, in our likeness"
Genesis 1:26

Rationale

At Marlow Church of England Infant School our curriculum vision is to inspire learning and ignite curiosity within a welcoming Christian and spiritual community. We embrace the uniqueness of everybody and are inclusive of all. Our values of respect, kindness, perseverance, forgiveness, thankfulness and service guide all that we do and our aim is for every child to feel nurtured, supported and safe.

Our belief is that every individual is created in God's image and therefore is precious and valuable. We believe in treating everybody with respect and dignity because we acknowledge everyone's God given value and unique identity

We aim to achieve this by providing children with the opportunity to work towards achieving their full potential by:

- Embracing the uniqueness of everybody and be inclusive of all
- Empowering all to be enthusiastic learners
- Ensuring that every child feels nurtured, supported and safe
- Enriching learning through progressive teaching methods and technology
- Being responsible to and for society
- Being good citizens of the planet

As a school we support the rights of children and these rights are encompassed in UN Convention of the Rights of the Child. This policy focuses on helping to realise Article 19*: You have the right to be protected from being hurt and mistreated, in body or mind* and Article 28: *You have the right to a good quality education.*

Introduction

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

This Acceptable Use Policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of ICT in their everyday work.
- The school will try to ensure that staff and volunteers will have good access to ICT to enhance their work, to enhance learning opportunities for pupils learning and will, in return, expect staff and volunteers to agree to be responsible users.

Staff/Volunteer Acceptable Use Agreement

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

For my professional and personal safety:

- I understand that Marlow C of E Infant School will monitor my use of the ICT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of school ICT systems (eg laptops, email, etc) out of school, and to the transfer of personal data (digital or paper based) out of school.
- I understand that the school IT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

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

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

The school has the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

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

- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings unless agreement has been sought from the Designated Safeguarding Lead/Headteacher and/or TurnITon
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School's Data Protection Policy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based Protected and Restricted data must be held in lockable storage.
- I understand that data protection policy requires that any staff or student data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

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

- I understand that this Acceptable Use Policy applies not only to my work and use of school IT equipment in school, but also applies to my use of school IT systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school / academy
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to the School Governors and in the event of illegal activities the involvement of the police.

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

Staff / Volunteer Name

Signed

Date

Date of Policy: January 2025

Date of review: January 2028

Appendix III

Acceptable Use Agreement for Community Users

This Acceptable Use Agreement is intended to ensure:

- that community users of school digital technologies will be responsible users and stay safe while using these systems and devices
- that school systems, devices and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that users are protected from potential risk in their use of these systems and devices

I understand that I must use school systems and devices in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems, devices and other users. This agreement will also apply to any personal devices that I bring into the school

- I understand that my use of school systems and devices and digital communications will be monitored
- I will not use a personal device that I have brought into school for any activity that would be inappropriate in a school setting.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.
- I will not access, copy, remove or otherwise alter any other user's files, without permission.
- I will ensure that if I take and/or publish images of others I will only do so with their permission. I will not use my personal equipment to record these images, without permission. If images are published it will not be possible to identify by name, or other personal information, those who are featured.
- I will not publish or share any information I have obtained whilst in the school on any personal website, social networking site or through any other means, unless I have permission from the school.
- I will not, without permission, make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a school device, nor will I try to alter computer settings, unless I have permission to do so.
- I will not disable or cause any damage to school / academy equipment, or the equipment belonging to others.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).
- I understand that if I fail to comply with this Acceptable Use Agreement, the school / academy has the right to remove my access to school systems / devices

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

Name

Signed

Date

Appendix IV

Children's Acceptable Internet Use Policy

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

This acceptable use policy is intended to ensure:

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

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

This policy will help me to be safe.

- I will keep the rules to help me stay safe; this will make me a responsible user.
- I will take care of the equipment that we have in school.

For my safety:

- I will not tell anyone my password.
- I will remember 'stranger danger' when I use the internet.
- When I am on the internet I will not tell anyone about myself.
- I will tell a grown up straight away about anything that makes me feel uncomfortable.

I will consider other people when on the internet:

- I will be polite and responsible when I communicate with others online.
- I will not take or share pictures of other children.

I will look after school equipment:

- I will only use the equipment that the teacher says I should use.
- I will tell an adult if the equipment is broken or not working.
- I will only open emails and attachments when my teacher says it is ok to do so.
- I will not alter computer settings on purpose.

When I use the internet:

- I will only go on the websites that my teacher has told me to use.
- I should remember that information on the internet may not be true.

I know I have to be sensible, both in and out of school:

- If I break the rules I know that I might not be allowed to use the school resources.

Class…… Date……

Appendix V

Online safety Resources

For School and Home

National College
https://nationalcollege.com/enrol/marlow-c-of-e-infant-school

Smartie the Penguin, Think before you click!
https://www.childnet.com/resources/smartie-the-penguin

CEOP – Think you know
https://www.thinkuknow.co.uk/

Safer Internet Day
https://saferinternet.org.uk/safer-internet-day/safer-internet-day-2025

National Centre for Computing Education (NCCE)
https://teachcomputing.org/

UK Council for Internet Safety
https://www.gov.uk/government/organisations/uk-council-for-internet-safety

Education for a Connected World
https://www.gov.uk/government/publications/education-for-a-connected-world

For Parents

NSPCC - Online safety
https://www.nspcc.org.uk/keeping-children-safe/online-safety/

Parent Zone
https://parentzone.org.uk/parent-info

Internet Matters
https://www.internetmatters.org/schools-esafety/parent-online-support-pack-teachers/

National College for webinars and information about #WakeUpWednesday online safety newsletter
https://nationalcollege.com/enrol/marlow-c-of-e-infant-school

Date reviewed: January 2025

Review Date: January 2028