Red Marsh School Online Safety Policy

This policy applies to all members of Red Marsh School community who have access to and are users of school ICT systems, both in and out of Red Marsh School.

The education of pupils in online safety is an essential part of Red Marsh School's safeguarding provision. Our pupils, all of whom have learning difficulties, need the help and support of Red Marsh School staff to recognise and avoid online safety risks and build their resilience and understanding when using technology. Our parents/carers may also need support to help their child to avoid online safety risks. This policy should be read in conjunction with the policies outlined in the appendix.

Rachel Dixon is the on line safety lead.

The use of technology in Education

Education – Pupils

Our Online Safety Curriculum

Our curriculum encourages pupils to be helped to adopt safe and responsible use both within and outside school through:

- Key online safety messages reinforced at all possible opportunities across the whole curriculum
- Individual on line safety targets set according to pupils' individual needs
- A planned online safety curriculum, including cyberbullying and sexting is taught as part of the Computing and PSHCE curriculum, including SRE.

Online safety includes pupils being supported to build resilience to radicalisation
(See Radicalisation and Extremism Policy)

Our key safeguarding message

Our key safeguarding message, including on-line safety is:

"Speak out, stay safe, tell or show a trusted adult."

We aim for pupils to be able to identify at least one trusted adult building to five trusted adults for our more able students.

In addition we will work with identified pupils as part of their personalised learning intention targets to re-inforce additional safety messages these include

Things we must do online:

- We tell a trusted adult if we see or hear something that worries us, scares us or makes us sad.
- Tell an adult when we are online
- Be kind when we are on line

Things we do not do on line

- We must not make friends on line and never meet anyone from online
- We must not share our personal information on line **(**What is personal information? Our name? Where we live? Our school?)
- We must not search inappropriate sites (staff will talk to pupils about what is an acceptable or unacceptable site within school).

As a school we consult with our pupils, through the school council, in order to find out if they feel safe within school. This includes feeling safe online. We also know each of our pupils extremely well and where appropriate discuss with them online safety issues.

Staff responsibility when supporting pupils using technology across the curriculum

Staff must:

- Ensure when pupils are using technology they are supervised by adults at all times
- Act as good role models in their use of digital technologies, the internet and mobile devices.
- In lessons where internet use is pre-planned teachers must check that sites are suitable for use by pupils. For good educational reasons, students may need to research topics (e.g. racism, drugs, and discrimination) that would normally result in searches being blocked. In such a situation, staff can request that the ICT technician can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.
- Follow the acceptable users' guidance if they are made aware that a pupil has tried to carry out a search on in appropriate topic. See appendix 4.

Education – Parents / Carers

Red Marsh School will aim to build awareness for parents and carers about online safety through the sharing of information. This will include information on the school website, individual meetings with parents/carers and sharing of online information for example

offering parent workshops. Parents will be informed through the online safety policy and parental letters of the acceptable users guidance. See appendix 4.

Education – The Wider Community

Red Marsh School website provides online safety information that can be accessed by the wider community.

Education & Training – Staff / Volunteers

All staff will receive online safety training to enable them to understand their responsibilities, as outlined in this policy.

Training will be offered as follows:

- All new staff will receive online safety training as part of their induction programme
- All staff will read the Online Safety Policy, Acceptable Use Policy and the Safer Working Practice document. All staff will sign to say they have read and understood these documents.
- All staff will be regularly updated and online safety messages reinforced during staff and/or morning meetings.
- The Online Safety Lead, will provide advice or organise training to individuals as required.
- The Online Safety Lead will receive regular updates through attendance at external training events and/or by reviewing guidance documents released by relevant organisations.

Training – Governors

Health and Safety governors and the Online Safety governor, Pat Naylor, will be provided with information relating to online safety.

Technical aspects of on line safety

Red Marsh School's technical systems will be managed in ways that ensure the schools network is as safe and secure as is reasonably possible and meets recommended technical requirements.

Security

- BT Lancashire Broadband service security measures are in place to protect the system from accidental or malicious attempts which might threaten the security of the schools systems and data. These are tested regularly. Red Marsh School infrastructure and individual workstations are protected by up to date anti-virus software.
- The wireless systems and cabling is securely located.
- School devices that are used out of school must be used in an appropriate manner linked to the educations of the pupils or safeguarding. See table 1 for the extent of personal use.

Filtering

- Red Marsh School has a service level agreement for Filtering provided by BT Lancashire Services (BTLS) Light Speed.
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by BTLS light speed.
- Content lists are regularly updated and internet use logged and regularly monitored by the ICT technician Stewart Atkin and Online Safety Lead (OSL).
- Internet filtering should ensure that children are safe from terrorist and extremist material when accessing the internet.
- Red Marsh School has differentiated user-level filtering for staff and pupils
- The process for requesting filtering change is to report to the OSL who will then ask the ICT technician to make the changes.

Password protection

- All users will have clearly defined access rights to school systems and devices. Log in with a username and password
- All classes will be provided with a username and secure password by ICT technician who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password.
- The "master / administrator" passwords for Red Marsh School, is held by BT Lancashire and the ICT technician and must also be available to the Headteacher
- Personal data used for the role of teaching should be as far as possible kept secure
- Agreed procedures are in place for the provision of temporary access of "guests" (eg trainee teachers, supply teachers, visitors) onto Red Marsh School systems. These include a signing the relevant Acceptable Users Policy (AUP) and receiving a temporary password. Kept by ICT technician and OSL.

Monitoring and reporting

- There will be regular reviews and audits of the safety and security of Red Marsh school's technical systems
- The ICT technician regularly monitors and records the activity of users on Red Marsh School technical systems and users are made aware of this in the Acceptable Use Agreement.
- **Reporting -** Technical incidents to be reported to the ICT Technician Stewart Atkins and or Rachel Dixon. Any **safeguarding issues to be reported to the DSL's Catherine Dellow and or Jenny Slater.**

Mobile Technologies

Use of digital and video images

Pupils and Staff

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites and sexting.
- Staff and volunteers are allowed to take digital images to support educational aims. Those images must **ONLY** be taken on school equipment. NO personal equipment belonging to staff should be used for recording images of children.
- Care should be taken when taking digital images that pupils are appropriately dressed and are not participating in activities that might bring Red Marsh School into disrepute.
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Staff must check with the school office for consent to share, distribute and publicise those images.
- Pupils' full names will not be used anywhere on a website or Facebook, particularly in association with photographs.
- Pupils can only take images as part of a lesson and under the supervision of an adult, they will not share , publish or distribute these images

Parents / Carers

- Written permission from parents or carers will be obtained before photographs of pupils are published on Red Marsh School website / social media / local press. This will be updated annually.
- Parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images if they have other children on must **not** be made publicly available on social networking sites.
- Parents carers are asked to sign to say they are taking videos and digital images

Data Protection

Red Marsh School will ensure Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data where possible using encryption and secure password protected devices.
- When personal data is stored on any portable computer system, memory stick or any other removable media it is essential that staff as far as possible ensure data is protected.

Communications

The following table provides information on the acceptable use of communication using technology:

	Staff & other Adults in school				Students / Pupils			
Communication Technologies (Including 3G & 4G technologies)	Allowed	Allowed at certain times	Allowed for selected	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school	✓				✓[1]	✓[2]		
Use of personal mobile phones in lessons				✓				✓
Use of mobile phones in social time		✓[3]						✓
Taking photos on mobile phones / or personal cameras				✓				✓
Use of other mobile devices e.g. tablets, gaming devices		✓					✓	
Use of personal email addresses in school, or on school network				✓				✓
Use of school email for personal emails				✓				✓
Use of messaging apps				✓				✓
Use of social media		✓						✓

Safer working practices for staff

- There must be **No** personal digital communication between staff and students
- Any digital communication between staff parents / carers can only take place using the official school communication systems i.e. school email or school text service. Unless staff are out of school and they need to make an emergency call to school or a parent.
- Red Marsh schools email service is regarded as safe and secure and is monitored. Users should be aware that email communications may be monitored.
- As part of planned lessons class email addresses can be provided for educational use.
- Staff should not use personal emails for work communications
- Staff, visitors and volunteers must immediately report, to the headteacher the receipt of any communication that makes them feel uncomfortable from parents, colleagues and pupils, is offensive, discriminatory, threatening or bullying in nature and must not

[1] Senior students only allowed mobiles to and from school but locked away during day.
[2] FE students able to use school mobile phone as part of their independence training when agreed by the teacher
[3] **Staff must keep their mobile phone and other mobile devices in their locker and used only during break times but never in the presence of pupils**

respond to any such communication. This is reported to the headteacher as it is a personnel issue.

Social Media procedures

The School

Red Marsh School permits reasonable and appropriate access to private social media sites, however this must only take place during official staff breaks and never in the presence of pupils. If personal use of social media is considered to be interfering with relevant duties, disciplinary action will be taken

- Red Marsh School provides the following measures to ensure reasonable steps are in place to minimize risk of harm to pupils, staff and Red Marsh School through:
- Ensuring that personal information is not published, however governor information is published on the Red Marsh School website as required by DFE
- Training is provided through induction and regular updates regarding: acceptable use; social media risks, Safer Working Practice; checking of settings; data protection; reporting issues.
- Clear reporting guidance i.e. reports to be made to the SLT, any abuse and misuse will be dealt with under school disciplinary procedures or safeguarding procedures
- As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about Red Marsh School

School staff

School staff should ensure that:

- No reference is made in their personal social media to the pupils, parents / carers or school staff in relation to their work at school or can be traced back to their role in school
- Comments do not bring Red Marsh school into disrepute
- Personal opinions cannot be attributed to Red Marsh School or the local authority
- Security settings on personal social media profiles are regularly checked to ensure privacy settings are of the highest setting. If staff do not know how to ensure highest privacy settings they should seek advice from Stuart, Jenny Slater or Rachael Dixon
- They do not use technology to harass, cyberbully, discriminate on the grounds of sex, race or disability or defame a third party
- Where a personal account is used which associate itself with Red Marsh School, it must be made clear that the member of staff is not communicating on behalf of Red Marsh

School with an appropriate disclaimer. Such personal communications are within the scope of this policy

Personal communications which do not refer to or impact upon Red Marsh School are outside the scope of this policy

Official school Facebook site procedures:

- The headteacher approves all postings
- The Assistant headteacher Jenny Slater and the admin lead Cheryl Wood are responsible for posting
- The Facebook Site will be for sharing information not for dialogue with a parent or carers
- Any negative posts will be screen shot and removed from the site
- Any abuse or misuse will be reported to the LCC legal team
- Incidents relating to staff may be dealt with under school disciplinary procedures
- The school Facebook site will be monitored by the online governor

Unsuitable / inappropriate use of technology

The school

Cyber-bullying or other Online Safety incidents, which may take place outside of Red Marsh School are dealt within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate Online Safety behaviour that take place in and out of school. See appendix 4.

School Actions & Sanctions

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

Pupil Incidents

<table>
<tr><th>Incident</th><th>Procedure and Sanctions</th></tr>
<tr><td>Accidental access to inappropriate materials.</td><td>Child to tell a trusted adult
Minimise the webpage or turn the monitor off button.
Adult will inform OSL
Enter the details in the Incident Log OSL may report to ICT technician who will the report to BTLS filtering services if necessary.
Persistent ‘accidental’ offenders may need further action.</td></tr>
<tr><td>Using other people’s logins and passwords maliciously.</td><td rowspan="4">Inform OSL
Enter the details in the Incident Log.
Additional awareness raising of online safety issues with individual child
Parent/carer involvement
More serious or persistent offences may result in further action in line with Behaviour Policy.</td></tr>
<tr><td>Deliberate searching for inappropriate materials.</td></tr>
<tr><td>Bringing inappropriate electronic files from home.</td></tr>
<tr><td>Using chats and forums in an inappropriate way.</td></tr>
</table>

Staff Incidents

Red Marsh School believes that the activities referred to in appendix 1 would be inappropriate in a school context and that (user) staff should not engage in these activities in or outside Red Marsh School when using school / equipment or systems.

If there are any incidents they are reported to the OLS the flow chart will be used to identify actions .Staff should be aware that actions may be dealt with through normal disciplinary procedures or may lead to referral to LADO, police, warning, suspension or further disciplinary action.

If there is any suspicion that the concerns may contain child abuse images, or if there is any other suspected illegal activity, refer to Flowchart (appendix) for responding to online safety incidents and report immediately to the police.

Related Policies:

This policy should be read in conjunction with the schools safeguarding, ICT acceptable users, behavior policies and Code of conduct.

Monitoring the impact of the policy

Red Marsh School will monitor the impact of the policy using:

- Logs of reported incidents
- Daily Learning Walks
- Monitoring logs of internet and network activity (including sites visited) / filtering to be supplied by Stewart Atkin our ICT technician to our OSL.

Further information

This Online Safety policy has been developed by an online safety group made up of:

- Head teacher and DSL – Catherine Dellow
- Online Safety Lead - Rachel Dixon
- Health and Safety governor committee comprising of SLT, Teacher, Support Staff and parent governors
- Key online safety governor Pat Naylor
- ICT Technician – Stewart Atkin

The development of the policy has also been supported by the PSD and Computing subject leaders.

Staff roles and responsibilities for the implementation and monitoring of the policy can be found in appendix 3

Schedule for Monitoring and Review of the policy

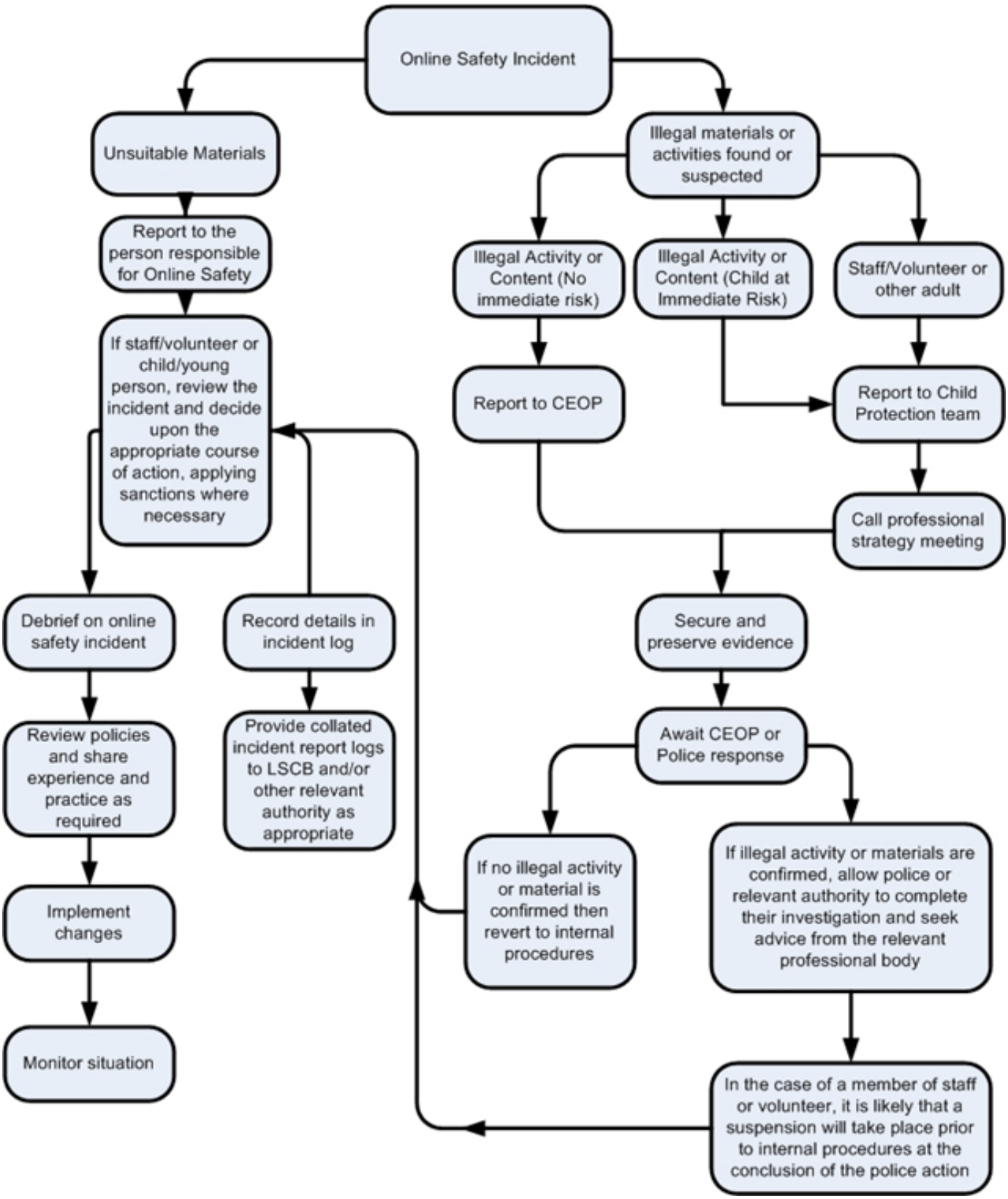
This Online Safety policy is approved by the Health Safety Governor committee	26/04/2017 Issue 2 20/12/18
The implementation of this Online Safety policy will be monitored by:	Online Safety Lead – Rachel Dixon
Monitoring will take place at regular intervals:	Daily learning walks
Governors Health and safety Sub Committee will receive a report on the implementation of the Online Safety Policy generated by Online Safety Lead (which will include anonymous details of online safety incidents) at regular intervals:	Termly
The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	Annually 26/04/2017 Issue 2 20/12/2018
Should serious online safety incidents take place, the following external persons / agencies should be informed:	LA Safeguarding Lead- Tammy Tywang LADO- Tim Booth Police

Appendix 1 - Appropriate and in appropriate use of technology. This refers to using school equipment or your own devices within the school premises

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

Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by Red Marsh School / academy				X	
Infringing copyright				X	
Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)				X	
Creating or propagating computer viruses or other harmful files				X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)				X	
On-line gaming (educational)		X			
On-line gaming (non-educational)		X			
On-line gambling				X	
On-line shopping / commerce		X			
File sharing		X			
Use of social media		X			
Use of messaging apps		X			
Use of video broadcasting e.g. Youtube		X			

Appendix 2 –Flow chart for online safety incidents



Roles and Responsibilities (appendix 3)

The following section outlines the online safety roles and responsibilities of individuals and groups within Red Marsh School.

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 Health and safety Governors committee receiving regular information about online safety incidents and monitoring reports.

Pat Naylor Safeguarding Governor and Chair of Governors has taken on the role of Online Safety Governor she will also receive regular information about online safety incidents and monitoring reports.

The role of the Online Safety Governor will include:

- Termly meetings with the Online Safety Lead which will include feedback of online safety incident logs and filtering
- Receiving minutes from the Health and Safety committee
- Regular monitoring of implementation of policy
- Reporting to full Governors as part of the safe guarding report

Online Safety Group

The Online Safety Group provides a consultative group that has wide representation from Red Marsh School, with responsibility for issues regarding online safety and the monitoring the Online Safety Policy including the impact of initiatives.

Members of the Online Safety Group will assist the Online Safety Lead with: the production , review and monitoring of Red Marsh School Online Safety Policy.

Head teacher:

The Head teacher has a duty of care for ensuring the safety (including online safety) of members of Red Marsh School community, though the day to day responsibility for online safety will be delegated to the Online Safety Lead.

- The Head teacher and the deputy head teacher (DSL/OSL) are aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. (appendix 2) on dealing with online safety incidents.
- The Head teacher is responsible for ensuring that the Online Safety Lead and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues.

- The Head teacher will ensure that there is a system in place to allow for monitoring and support for those in school who carry out the internal online safety monitoring role. This will be provided by the head teacher and Chair of Governors the online safety governor
- The Senior Leadership Team will receive regular monitoring reports from the Online Safety Lead as part of the governor Health and Safety committee

Online Safety Lead:

- Rachel Dixon takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing Red Marsh School online safety policies
- Ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place
- Organise training for staff
- Liaises with the Local Authority
- Liaises with school technical staff
- Receives reports of online safety incidents and creates a log of incidents to inform future online safety developments
- Meets termly with Online Safety *Governor* to discuss current issues, review incident logs and filtering / change control logs
- Attends or submits a report to the Health and Safety committee of *Governors*
- Reports regularly to the head teacher.

ICT Technician
The ICT Technician is responsible for

- Ensuring ICT Technical support is provided by BT Lancashire Services.
- Liaising with Computing Subject Leader and OSL Rachel Dixon.
- That the wireless systems and cabling are securely located.
- The Online Safety lead and ICT Technician are responsible for managing the security of Red Marsh School network.
- Red Marsh School systems are kept up to date in terms of security by the ICT Technician.
- Only designated users, such as Computing Subject Leader, ICT Technician and identified staff are allowed to download files or install software.
- Ensuring Red Marsh School's *t*echnical infrastructure is secure and is not open to misuse or malicious attack

- Ensuring Red Marsh School meets required online safety technical requirements and any Local Authority Online Safety Guidance that may apply.
- Supporting users to access the networks and devices through a properly enforced password protection.
- The filtering system, is applied and updated on a regular basis and that its implementation is supported by the Online Safety lead
- The use of the network, internet, are regularly monitored in order that any misuse, attempted misuse can be reported to the Online Safety Lead and Head teacher or relevant authority for investigation / action / sanction

Staff
Are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current Red Marsh 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 Online Safety Lead for investigation
- all digital communications with parents / carers should be on a professional level and only carried out using official school systems i.e. text messages or emails.
- online safety issues are embedded in all aspects of the curriculum and other activities
- pupils are safe when online staff must monitor pupils when they are using digital technologies,
- in lessons where internet use is pre-planned pupils must be guided to sites checked as suitable for their use.
- If any unsuitable material is found staff must minimise the image or information and report to OSL.

Will be trained in Online Safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming, cyberbullying and sexting
- Child Sexual Exploitation (CSE)
- Radicalisation

Pupils, as far as possible:

- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- use Red Marsh School digital technology systems in accordance with classroom rules
- use technology only in the presence of an adult
- have a growing understanding of research skills and are supported to uphold copyright regulations
- Supported to follow Red Marsh Schools safeguarding policies on the use of mobile devices, digital cameras, use of images and cyber-bullying.
- should understand the importance of adopting good online safety practice when using digital technologies 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. Red Marsh School will take opportunities to help parents understand these issues through individual parent meetings, the website and sharing of on line information for example offering parent workshops. Parents and carers will be encouraged to support Red Marsh School in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website including Facebook
- on-line pupil records
- their children's personal devices in Red Marsh School

Appendix 4

Online Safety (Acceptable User Statement) shared with parents

As a school we are constantly working to safeguard your child. As part of our work to safeguard pupils on line, pupils are always supervised when using the computers and i-pads. The school also has filtering/blocking system to prevent pupils accessing unsuitable materials. However, sometimes our more able students are curious and may try to search for unsuitable

material before a member of staff is aware. As a school we run specialist reports to see which sites have been blocked, if we identify a pupil has been trying to search for unsuitable materials we have the following procedures in place:

1) Staff will explain to the pupil that they must not search for the unsuitable subject
2) Parents/carers will be made aware so that they can support their child to understand that these searches are not appropriate and can ask for advise on how to prevent pupils accessing such sites at home.
3) If a pupil continues to try to search unsuitable sites they will be prevented from using the i-pad or the computer for a week.