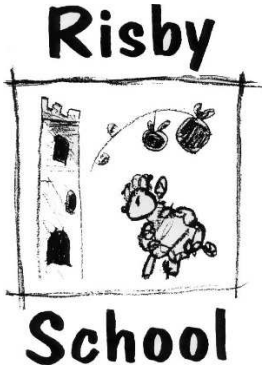


Risby CEVC Primary School

Online Safety Policy

Prepared by:	**Premises and Health & Safety Committee**
Approved by:	**Premises and Health & Safety Committee**
Signature of Chair of Premises and Health & Safety Committee:	
Date Approved:	**March 2019**
Review Date:	**March 2020**

Schedule for Development / Monitoring / Review

The implementation of this Online Safety policy will be monitored by the Designated Safeguarding Lead (DSL), the Online Safety Lead and the Safeguarding Governor.	Designated Safeguarding Lead, Online Safety Lead and Safeguarding Governor
Monitoring will take place at regular intervals:	Annually
The Governing Body will receive a report on the implementation of the Online Safety Policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals:	Annually and when necessary
The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	September 2019
Should serious online safety incidents take place, the following external persons / agencies should be informed:	Network Manager, Customer First, LADO, Police

Aims

Our aim in presenting an online safety policy is to create a safe environment where we can both work and learn. This environment should be safe for both young people and adults alike.

Online safety is not purely a technological issue. The responsibility for online safety must not be solely delegated to technical staff, or those with a responsibility for ICT, but must be part of a larger whole school approach to both keeping children safe and building resilience. Schools must therefore firmly embed online safety within all safeguarding policies and practices. This then makes that responsibility rest with of all those who work with young people whether in a paid or unpaid capacity.

The risks that our community faces can be summarised as follows:

Content

- Exposure to inappropriate content, including online pornography, ignoring age ratings in games (exposure to violence associated with often racist language), substance abuse.
- Lifestyle/well-being websites, for example pro-anorexia/self-harm/suicide sites.
- Hate sites.
- Content validation: how to check authenticity and accuracy of online content.

Contact

- Grooming.
- Online bullying in all forms.
- Identity theft - including 'frape' (hacking Facebook profiles) and sharing passwords.

Conduct

- Privacy issues, including disclosure of personal information.
- Digital footprint and online reputation.
- Health and well-being (amount of time spent online - internet or gaming).
- Sexting (sending and receiving of personally intimate images) also referred to as SGII (self-generated indecent images).
- Copyright (little care or consideration for intellectual property and ownership - such as music and film)

It is vital that children and young people are educated to be safe and responsible users capable of making good judgements about what they see, find and use.

The aims of this policy are therefore:

- To emphasise the need to educate staff, parents/carers and children and young about the safe use of technologies both within and outside the school setting;
- To provide safeguards and agreement for acceptable use to guide all users, whether staff or student, in their online experiences;

- To ensure adults and children are clear about procedures for misuse of any technologies both within and beyond the school setting;
- To develop links with parents/carers and the wider community ensuring input into policies and procedures with continued awareness of the benefits and potential issues related to technologies.

Scope

This policy applies to all members of Risby CEVC Primary School community (including staff, pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of school. The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of online bullying, or other online safety incidents covered by this policy, which may take place outside of 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. In the case of both acts, action can only be taken over issues covered by the published Behaviour policy.

The school will deal with such incidents 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 out of school.

Risby CEVC Primary School takes very seriously the naming of school staff in social media forums, such as Facebook and Twitter and, in particular, any comments that are deemed negative; call into question their professional integrity or have an impact on their well-being.

The policy also:

- Sets out the key principles expected of all members of the school community at Risby CEVC Primary School with respect to the use of ICT-based technologies.
- Safeguards and protects the children and staff of Risby CEVC Primary School.
- Assists school staff working with children to work safely and responsibly with the internet and other communication technologies and to monitor their own standards and practice.
- Sets clear expectations of behaviour and/or codes of practice relevant to responsible use of the internet for educational, personal or recreational use.
- Has clear structures to deal with online abuse such as online bullying which are cross referenced with other school policies.
- Ensures that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- Minimises the risk of misplaced or malicious allegations made against adults who work with students.

Communication

The policy will be communicated to staff/pupils/community in the following ways:

- Posted on the school website.
- Included as part of school induction pack for new staff.
- Age appropriate Online Safety Agreements will be signed and discussed with pupils at the start of each year.
- Home/School Agreements will be issued to the whole school community, usually on entry to the school, and held in pupil files.

Key Responsibilities

Online Safety Lead

- Takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policy;
- Facilitates training and advice for all staff;
- Promotes an awareness and commitment to online safety throughout the school community;
- Ensures online safety education is embedded across the curriculum;
- Liaises with ICT technical staff;
- Communicates regularly with SLT and the designated Online Safety Governor to discuss current issues, review incident logs and filtering checks;
- Ensures all staff are aware of the procedures that need to be followed in the event of an online safety incident;
- Ensures an Online Safety Incident Log is kept up-to-date;
- Liaises with the DSL, Local Authority and relevant agencies as necessary;
- Provides online safety advice and information to parents/carers.

Headteacher

- Takes overall responsibility for online safety provision;
- Takes overall responsibility for data and data security;

- Is the Senior Information Risk Officer (SIRO);
- Ensures the school uses an approved, filtered internet Service, which complies with current statutory requirements (EXA);
- Makes sure that another member of the Senior Leadership Team and the Online Safety Lead are aware of the procedures to be followed in the event of a serious online safety incident, including an allegation being made against a member of staff. (See the flowchart included in a later section-responding to Incidents of Misuse);
- Ensures access controls/encryption memory sticks exist to protect personal and sensitive information held on school-owned devices;
- Ensures the secure maintenance of an Online Safety Incident Log;
- Ensures the provision of individual log-ins for all staff and Key Stage 1 and 2 pupils;
- Receives regular monitoring reports from the Online Safety Lead;
- Ensures there is a system in place to monitor and support staff who carry out internal online safety procedures;
- Ensures appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster.

Designated Safeguarding Lead (DSL)
The DSL should be trained in online safety issues and be aware of the potential for serious child protection / safeguarding issues arising from:

- Sharing of personal data;
- Access to illegal / inappropriate materials;
- Inappropriate on-line contact with adults / strangers;
- Potential or actual incidents of grooming;
- Online-bullying;

The DSL should be aware that these are safeguarding issues, not technical issues, simply that the technology provides additional means for safeguarding issues to develop.

Network Manager
- Reports any online safety related issues that arise, to the Online Safety Lead;
- Ensures that users may only access the school's networks through an authorised and properly enforced password protection policy, in which passwords are regularly changed;
- Ensures that provision exists for misuse detection and malicious attack, e.g. keeping virus protection up-to-date;
- Maintains the security of the school ICT system, ensuring that the school's technical infrastructure is secure and is not open to misuse or malicious attack;
- Ensures the school meets required online safety technical requirements and any Local Authority Online Safety Policy Guidance that may apply;
- Ensures access controls exist to protect personal and sensitive information held on school-owned devices;
- Ensures the school's policy on web-filtering is applied and updated on a regular basis;
- Informs the Headteacher and the Online Safety Lead are informed of issues relating to filtering;
- Keeps up-to-date with the school's Online Safety Policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant;
- Ensures the use of the network/remote access/email is regularly monitored in order that any misuse/attempted misuse can be reported to the Headteacher and the Online Safety Lead/Headteacher for investigation action/sanction;
- Keeps up-to-date documentation of the school's online security and technical procedures;
- Provides individual log-ins for all staff and Key Stage 1 & 2 pupils.

Teachers
- Embed online safety issues in all aspects of the curriculum and other school activities;
- Supervise and guide pupils carefully when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant);
- Ensure pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content, such as copyright laws.

Staff
All staff have a responsibility to:
- Ensure they have read, understood and signed the Staff Acceptable Use Agreement (AUA);
- Ensure they have an up-to- date awareness of online safety matters and of the current school online safety policy and practices;
- Be aware of online safety issues related to the use of mobile phones, cameras and handheld devices and that they monitor their use and implement current school policies with regard to these devices;

- Report any suspected misuse or problem to the Online Safety Lead;
- Maintain an awareness of current online safety issues and guidance e.g. through CPD;
- Model safe, responsible and professional behaviours in their own use of technology;
- Ensure that any digital communications with pupils are on a professional level and only through official school-based systems, never through personal mechanisms or devices.

Pupils

All pupils must:

- Read, understand, sign and adhere to the Pupil Online Safety Agreement (as age appropriate);
- Develop good research skills and understand the need to avoid plagiarism and uphold copyright regulations;
- Understand the importance of reporting abuse, misuse or access to inappropriate materials;
- Know what action to take if they or someone they know feels worried or vulnerable when using online technology;
- Know and understand the school policy on the use of mobile phones, digital cameras and handheld devices;
- Know and understand the school policy on the taking/use of images and on cyber bullying;
- Understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school;
- Understand that the school will respond to any actions committed outside of school using digital technologies where their actions have an impact within school;
- Take responsibility for learning about the benefits and risks of using the internet and other technologies safely both in school and at home;

School Business Manager

- Ensures all data held on pupils on the school office machines has appropriate access controls in place.

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 Premises and Health & Safety Committee receiving regular information about online safety incidents and monitoring reports from the Online Safety Governor. The role of the Online Safety Governor includes:

- Regular meetings with the Online Safety Lead;
- Regular monitoring of online safety incidents;
- Reviewing and monitoring the school Online Safety Policy;
- Reviewing and monitoring the school filtering policy;
- Reviewing the online safety curricular provision: ensuring relevance, breadth and progression;
- Consulting stakeholders: including parents / carers and pupils about the online safety provision;
- Monitoring improvement actions identified through use of the 360 degree safe self-review tool;
- Reporting to the Full Governing Body;

Parents

Parents / Carers play a crucial role in the education of their children and in the monitoring / regulation of the children's online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond. This school will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities, including share sessions;
- Information leaflets in school newsletters and on the school website;
- Online Safety Parent Information Meetings;
- High profile events / campaigns e.g. Safer Internet Day;
- Reference to the relevant websites / publications;
- Introduction of the Home/School Agreements to new parents, to ensure that principles of safe online behaviour are made clear.

Parents and carers will be encouraged to support the school in promoting good online safety practice by:

- Supporting the school in promoting online safety and endorse the Parents' Home/School Agreement, which includes the pupils' use of the internet and the school's use of photographic and video images;
- Reading, understanding and promoting the school Pupil Online Safety Agreement with their children;

- Accessing the school website, Class Dojo and school-related Facebook groups in accordance with the relevant school agreement;
- Consulting with the school if they have any concerns about their children's use of technology.

External Groups

Any external individual/organisation will sign to say they have read and received this policy prior to using any equipment or the internet within school.

Education and Training

Pupils

The education of pupils in online safety is an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience. This school has a relevant age appropriate, progressive and creative online safety education programme as part of both the Computing and PSHE – Ready for Life curricula. It is built on national guidance covers a range of skills and behaviours appropriate to pupil age and experience. Education is provided through:

- The planned online safety curriculum is provided as part of the Computing curriculum (Autumn Term); Ready For Life: Internet Safety Week (Spring Term); Whole School Safety Week (Summer Term);
- Key online safety messages are also reinforced as part of a programme of PSHE assemblies;
- Pupils are taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information;
- Pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet;
- Pupils are supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making;
- Pupils of all ages are taught the importance of passwords and to know that these must be kept private;
- Children are taught the risks associated with downloading, posting or sharing information and chatting online;
- Pupils are taught acceptable online behaviour, how to report any abuse, including cyber bullying, and how to seek help if they experience problems when using the internet and related technologies;
- All pupils are taught about age appropriate (PEGI) gaming and older pupils are led to understand the issues around aspects of the commercial use of the internet including risks in pop-ups, buying online, online gaming and gambling;
- Staff remind students about their responsibilities and ensure that each child in Key Stage 1 & Key Stage 2 references their Online Safety Agreement whenever they go online;
- Staff act as good role models in their use of digital technologies, the internet and mobile devices;
- In lessons where internet use is pre-planned, pupils are guided to sites checked as suitable for their use.

Staff

All staff receive online safety training and understand their responsibilities, as outlined in this policy. The school:

- Makes regular training available to staff on online safety issues and the school's online safety education program; annual updates/termly staff meetings etc;
- Where applicable, identifies online safety as a training need within the performance management process;
- Provides, as part of the induction process, all new staff [including those on university/college placement and work experience] with information and guidance on the online safety policy;
- Ensures the Online Safety Lead receives regular updates through attendance at external training events;
- Presents this Online Safety Policy and its updates to staff in staff / team meetings / INSET days;
- Ensures staff know how to send or receive sensitive and personal data and understand the requirement to encrypt data where the sensitivity requires data protection.

Governors

Governors also take part in online safety training and awareness sessions, which are offered through:

- Attendance at training provided by the Local Authority / National Governors Association / or other relevant organisation;
- Participation in school training and information sessions for staff or parents.

Ensuring the Network is Used Safely

This school:

- Ensures staff read and sign that they have understood the school's Online Safety Policy. Following this, they are set-up with internet, email access and network access. Online access to service is through a unique, audited username and password;
- Ensures staff access to the schools' management information system is controlled through a separate password for data security purposes;
- Makes clear that no one should logon as another user and makes clear that pupils should never be allowed to logon or use teacher and staff logins, as these have far less security restrictions and inappropriate use could damage files or the network;
- Has set up the network with a shared work area for pupils and one for staff. Staff and pupils are shown how to save work and access work from these areas;
- Requires all users to log off when they have finished working or are leaving the computer unattended;
- Requires a user who finds a logged-on machine to log-off and then logon again as themselves. Users needing access to secure data are timed out after 15 minutes and have to re-enter their username and password to re-enter the network;
- Has set up the network so that users cannot download executable files/programmes;
- Has blocked access to music/media download or shopping sites – except those approved for educational purposes;
- Scans all mobile equipment with anti-virus/spyware before it is connected to the network;
- Makes clear that staff are responsible for ensuring that all equipment that goes home has up-to-date anti-virus and spyware software installed;
- Makes clear that staff are responsible for ensuring that any computer or laptop loaned to them by the school is used solely to support their professional responsibilities and that they notify the school of any "significant personal use" as defined by HM Revenue & Customs;
- Maintains equipment to ensure Health and Safety is followed e.g. projector filters cleaned, equipment is installed and checked by approved suppliers/LA electrical engineers;
- Ensures that access to the school's network resources from remote locations by staff is restricted and access is only through school/LA approved systems;
- Does not allow any outside agencies to access our network remotely except where there is a clear professional need and then access is restricted and is only through approved systems; e.g. technical support;
- Makes clear responsibilities for the daily back up and finance systems and other important files;
- Has a clear disaster recovery system in place for critical data that includes a secure, remote back up of critical data that complies with external Audit's requirements;
- Uses the DfE secure website for all CTF files sent to other schools;
- Ensures that all pupil level data or personal data sent over the internet is encrypted or only sent within the approved secure system in our LA secure file exchange;
- Follows advice on Local Area and Wide Area security matters and firewalls and routers have been configured to prevent unauthorised use of our network;
- Secures its wireless network to industry standard Enterprise security level/appropriate standards suitable for educational use;
- Ensures all computer equipment is installed professionally and meets health and safety standards;
- Ensures projectors are maintained so that the quality of presentation remains high;
- Reviews the school ICT systems regularly with regard to health and safety and security.

Password Policy

This school makes it clear that staff and pupils must always keep their password private, must not share them with others and must not leave them where others can find them.

- All staff have their own unique username and private passwords to access school systems;
- Staff are required to use STRONG passwords;
- Staff are required to regularly change their passwords into secure systems such as emails;
- All pupils in Key Stage 1 & Key Stage 2 have individual passwords.

Email

This school:

- Provides staff with an email account for their professional use and makes clear personal email should be through a separate account;
- Will contact the police if one of our staff or pupils receives an email that we consider is particularly disturbing or breaks the law;
- Will ensure that email accounts are maintained and up-to-date;
- Will report messages relating to or in support of illegal activities to the relevant authority;

- Knows that spam, phishing and virus attachments can make emails dangerous. We use a number of technologies to help protect users and systems in the school, including desktop anti-virus products, direct email filtering for viruses, trojans, pornography, phishing and inappropriate language.

Email: Pupils
Pupils may be introduced to and use email as part of the ICT/Computing scheme of work. Pupils are taught about the safety and 'netiquette' of using email both in school and at home and are taught:

- Not to give out their email address unless it is part of a school managed project or to someone they know and trust and is approved by their teacher or parent/carer;
- That an email is a form of publishing where the message should be clear, short and concise;
- That any email sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper;
- Not to reveal private details of themselves or others in email, such as address, telephone number;
- To 'Stop and Think Before They Click' and not open attachments unless sure the source is safe;
- To think carefully before sending any attachments;
- That embedding adverts is not allowed;
- That they must immediately tell a teacher/responsible adult if they receive an email which makes them feel uncomfortable, is offensive or bullying in nature;
- Not to respond to malicious or threatening messages;
- Not to delete malicious of threatening emails, but to keep them as evidence of bullying;
- Not to arrange to meet anyone they meet through email without having discussed with an adult and taking a responsible adult with them;
- That forwarding 'chain' email letters is not permitted;

Email: Staff
All staff sign a form to confirm that they have read our Online Safety Policy and understood the online safety rules, including email. We explain that:

- Staff must only use the email systems for professional purposes;
- Access in school to external personal email accounts may be blocked;
- An email sent to an external organisation must be written carefully, (and may require authorisation), in the same way as a letter written on school headed paper;
- The sending of multiple or large attachments should be limited and may also be restricted by the provider of the service being used;
- The sending of chain letters is not permitted;
- Embedding adverts is not allowed.

School Website
The Headteacher takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained.

- Uploading of information is restricted to authorised website user e.g. administrative staff and teachers;
- The school website complies with the statutory DfE guidelines for publications;
- Most material is the school's own work. Where other's work is published or linked to we credit the sources used and state clearly the author's identity or status;
- The point of contact on the website is the school address, telephone number and we use a general email contact address, e.g.admin@risby.suffolk.sch.uk. Home information or individual email identities are not published;
- Photographs published on the web do not have full names attached;
- Pupils' names are not used when publishing images to the school website.
- Teachers using school approved blogs or wikis are expected to password protect them and to run them from the school website.

Social Media
Teachers are instructed not to run social network spaces for student use on a personal basis or to open up their own spaces to their students or any parents, but to use the schools' preferred system for such communications.

- Staff will ensure that, in private use, no reference is made in social media to students/pupils, parents/carers or school staff;
- Messages and comments will not be made to any parent in the school on any social networking site;
- Staff will not engage in online discussion on personal matters relating to members of the school community;
- Personal opinions will not be attributed to the school or local authority;

- Security settings on personal social media profiles will be regularly checked to minimise risk of loss of personal information.

Monitoring of Public Social Media

- As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the school;
- The school's use of social media for professional purposes will be checked regularly by the Headteacher and Online Safety Lead to ensure compliance with the school policies.

Video Conferencing

This school only uses approved or checked webcams agreed by the Online Safety Lead/Headteacher.

Equipment and Digital Content

Mobile phones or personal mobile devices brought into school are entirely at the owner's own risk. The School accepts no responsibility for the loss, theft or damage of any phone or handheld device brought into school.

Pupil Use of Mobile Devices

The School strongly advises that mobile phones should not be brought into school by pupils.

- The school accepts that there may be particular circumstances in which a parent wishes their child to have a mobile phone for their own safety;
- Any mobile phone brought into school by a pupil must be turned off and stored with the Reception office on arrival at school;
- If a student breaches the school policy then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to parents or carers in accordance with the school policy.

Staff Use of Mobile Devices

- Any permitted images or files taken in school must be downloaded from the device and deleted as soon as possible;
- Normal telephone communication on school business should take place using the school's telephone. Staff are not advised to use their own mobile phones or devices for contacting or responding to children, young people or their families within or outside of the setting in a professional capacity, unless there are exceptional circumstances, which have been agreed by a member of the senior leadership team;
- Staff must not give their home or mobile telephone number to pupils or parents;
- Staff must not enter into instant messaging communications with pupils or parents;
- Mobile phones and personally-owned devices will be switched off or switched to 'silent' mode when in school. Bluetooth communication should be 'hidden' or switched off and mobile phones or personally-owned devices will not be used during teaching periods unless permission has been granted by a member of the Senior Leadership Team in emergency circumstances;
- Where staff members are required to use a mobile phone for school duties, for instance in case of emergency during offsite activities, or for contacting students or parents, they should use their own device and hide (by inputting 141) their own mobile number for confidentiality purposes. Wherever possible, staff should contact the School Office, who will then contact parents etc.

Digital Images and Videos

In this school:

- We gain parental/carer permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter/son joins the school;
- We do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials/DVDs;
- Staff sign the school's Acceptable Use Policy and this includes a clause on the use of mobile phones/personal equipment for taking pictures of pupils;
- The school blocks/filter access to social networking sites or newsgroups unless there is a specific approved educational purpose;
- Pupils are taught about how images can be manipulated in their online safety education programme and also taught to consider how to publish for a wide range of audiences, which might include governors, parents or younger children as part of their ICT scheme of work;
- Pupils are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information;
- Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location, such as house number, street name or school. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse;

- Parents may take photographs of their own child during performances unless there is safeguarding reason e.g. a looked after child in the school. At every performance parents will be reminded of use of photographs, including not to be downloaded on social networking sites.

Incident Management

The school believes that the following activities would be inappropriate in a school context and that users, as defined below, should not engage in these activities in / or outside the school when using school equipment or systems. The school policy restricts usage as follows:

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 the school or brings the 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 the school / academy					X	
Infringing copyright					X	
Revealing or publicising confidential or proprietary information (eg 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	

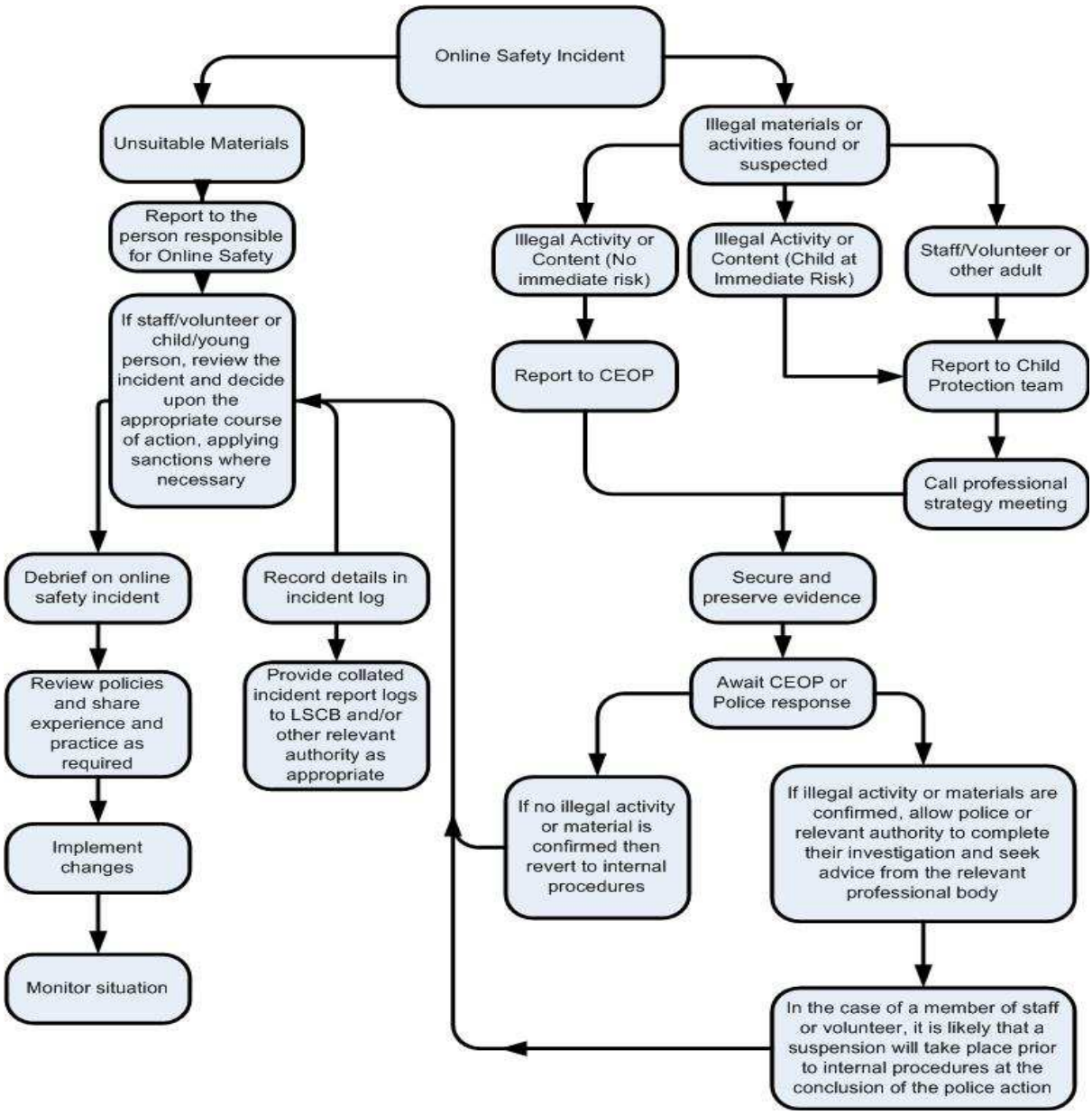
Responding to Incidents of Misuse

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

Illegal Incidents

If any apparent or actual misuse appears to involve illegal activity i.e:

- Child sexual abuse images;
- Adult material which breaches the Obscene Publications Act;
- Incidents of 'grooming' behaviour;
- The sending of obscene materials to a child;
- Adult material which potentially breaches the Obscene Publications Act;
- Criminally racist material;
- Promotion of terrorism or extremism;
- Other criminal conduct, activity or materials, then the following flowchart should be consulted and actions followed with particular reference to the sections on reporting the incident to the police and the preservation of evidence.



Other Incidents

If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (as described above) it is essential that the correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. More than one senior member of staff will be involved in the investigation which will be carried out on a

designated non- pupil computer. Staff will have appropriate internet access to conduct the procedure and the sites and content visited will be closely monitored and recorded.

The URL of any site containing the alleged misuse will be recorded and the nature of the content causing concern will be described. If necessary screenshots of the content on the machine that is being used for the investigation may be recorded and stored and then printed, signed and attached to the form. Parents/carers will be informed of online safety incidents involving young people for whom they are responsible.

Actions / Sanctions

Pupil Incidents	Refer to class teacher	Refer to Headteacher / Online safety Lead	Record in incident log	Refer to Police	Refer to technical support staff for action re filtering / security etc.	Inform parents / carers	Removal of internet access rights for a period of time	Warning	Further sanction e.g. exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	X	X	X	X		X	X		X
Unauthorised use of non-educational sites during lessons	X		X		X			X	Repeat offences
Unauthorised / inappropriate use of mobile phone / digital camera / other mobile device	X	X	X			X			X
Unauthorised / inappropriate use of social media / messaging apps / personal email	X	X	X		X	X		X	
Unauthorised downloading or uploading of files	X	X	X		X	X		X	
Allowing others to access school network by sharing username and passwords	X	X	X		X	X		X	
Attempting to access or accessing the school network, using another pupil's account	X	X	X		X	X	X	X	
Attempting to access or accessing the school network, using the account of a member of staff	X	X	X		X	X	X	X	
Corrupting or destroying the data of other users	X	X	X		X			X	
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	X	X			X			X
Continued infringements of the above, following previous warnings or sanctions	X	X	X			X	X		X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	X	X	X			X		X	
Using proxy sites or other means to subvert the school's filtering system	X	X	X		X	X	X		X
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X			X	X		X	
Deliberately accessing or trying to access offensive or pornographic material	X	X	X	X	X	X	X		X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	X	X	X					X	

Staff Incidents	Record in incident log	Refer to Headteacher Principal	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc.	Warning	Suspension
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	X	X	X	X			X
Inappropriate personal use of the internet / social media / personal email/instant messaging	X	X				X	
Unauthorised downloading or uploading of files	X	X			X	X	
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	X	X			X	X	
Careless use of personal data e.g. holding or transferring data in an insecure manner	X	X			X	X	
Deliberate actions to breach data protection or network security rules	X	X	X		X	X	
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	X	X	X		X	X	
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	X	X			X	
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with pupils	X	X	X			X	
Actions which could compromise the staff member's professional standing	X	X	X			X	
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	X	X	X			X	
Using proxy sites or other means to subvert the school's filtering system	X	X	X		X	X	
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X	X		X	X	
Deliberately accessing or trying to access offensive or pornographic material	X	X	X		X		X
Continued infringements of the above, following previous warnings or sanctions	X	X	X				X

Data Security

Data Protection

Personal data will be recorded, processed, transferred and made available according to the current data protection legislation. This school therefore ensures that:

- There is a regularly updated data protection policy;
- There is an appointed Data Protection Officer who is paid the appropriate ICO fee;
- It holds the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for;

- Data held is accurate and up to date and that inaccuracies are corrected without unnecessary delay;
- The lawful basis for processing personal data (including, where relevant, consent) has been identified and documented and details provided in a Privacy Notice;
- Where special category data is processed, a lawful basis and a separate condition for processing have been identified;
- Data Protection Impact Assessments (DPIA) are carried out;
- There are clear and understood arrangements for access to and the security, storage and transfer of personal data, including, where necessary, adequate contractual clauses or safeguards where personal data is passed to third parties e.g. cloud service providers;
- Procedures are in place to deal with the individual rights of the data subject i.e. a Subject Access Requests to see all or a part of their personal data held by the data controller;
- There are clear and understood data retention policies and routines for the deletion and disposal of data;
- There is a policy for reporting, logging, managing and recovering from an information risk incident which recognises the requirement to report relevant data breaches to the ICO within 72 hours of the breach, where feasible;
- There is a Freedom of Information Policy which sets out how it will deal with FOI requests;
- All staff receive data handling awareness / data protection training and are made aware of their responsibilities

Staff

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 using encryption and secure password protected devices;
- Encrypt and password protect any personal data that they store on a portable computer system, memory stick or any other removable media;
- Run approved virus and malware checking software on any portable computer system that they use;
- Securely delete data that they store on a portable computer system, memory stick or any other removable media once it has been transferred or its use is complete.

Managing the ICT Infrastructure

Internet Access, Security (Virus Protection) and Filtering

This school:

- Has the educational filtered secure broadband connectivity through EXA;
- Uses a filtering system which blocks sites that fall into categories such as pornography, race hatred, terrorism extremism, gaming, sites of an illegal nature etc. All changes to the filtering are logged and only available to staff with the approved 'web filtering management' status;
- Ensures the network is safe through the use of anti-virus software and the network is set-up so staff and pupils cannot download executable files;
- Uses DfE and LA approved systems, secured email to send personal data over the internet, encrypted devices (memory sticks) or secure remote access where staff need to access personal level data remotely;
- Blocks all chat rooms and social networking sites except those that are part of an educational network;
- Only unblocks other external social networking sites for specific purposes/internet Literacy lessons;
- Has blocked pupil access to music download or shopping sites;
- Uses security time-outs on internet access where practicable/useful;
- Works in partnership with its Network Managers to ensure any concerns about the system are communicated so that systems remain robust and protect students;
- Is vigilant in its supervision of pupils' use at all times, as far as is reasonable, and uses common-sense strategies in learning resource areas where older pupils have more flexible access;
- Ensures all staff and students have signed an Acceptable Use Agreement and read the Online Safety Policy and understand that they must report any concerns;
- Requires staff to preview websites before use [where not previously viewed or cached] and to ensure the curriculum context for internet use is matched to pupils' ability, using child-friendly search engines where more open internet searching is required, e.g. yahoo for kids or ask for kids, Google Safe Search;
- Is particularly vigilant when conducting 'raw' image search with pupils e.g. Google image search;
- Informs all users that internet use is monitored;
- Informs staff and students that that they must report any failure of the filtering systems directly to the Online Safety Lead and Network Managers;
- Provides advice and information on reporting offensive materials, abuse/bullying etc. available for pupils, staff and parents;
- Immediately refers any material that it suspects to be illegal to the appropriate authorities;
- Ensures that there are regular reviews and audits of school technical systems;

- Ensures that all servers, wireless systems and cabling are securely located and physical access restricted;
- Uses differentiated user-level filtering.

Asset Disposal

- Details of all school-owned software will be recorded in a software inventory;
- All redundant equipment will be disposed of through an authorised agency. This will include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data;
- All redundant equipment that may have held personal data will have the storage media forensically wiped. Alternatively, if the storage media has failed, it will be physically destroyed. The school will only use authorised companies who will supply a written guarantee that this will happen;
- Disposal of any equipment will conform to The Waste Electrical and Electronic Equipment Regulations 2006 and/or The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007.

Policies

The policies and guidance to help form safe environments to learn and work in include, but are not limited to:

- The School mobile phone and digital photography policy: Acceptable Use Policy
- The Staff Guidance for the Safer Use of the Internet.
- The Behaviour Management Policy.
- The Anti-Bullying Policy.
- The Staff Handbook/Code of Conduct for Staff.

Review and Monitoring

The Online Safety Policy is referenced from within other school policies: Child Protection Policy, Bullying policy and Behaviour policy.

- The school has an Online Safety Lead who will be responsible for document ownership, review and updates.
- The Online Safety Policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the school.
- The Online Safety Policy has been written by the school Online Safety Lead and Headteacher and is current and appropriate for its intended audience and purpose.

There is widespread ownership of the policy and it has been agreed by the SLT and approved by governors. All amendments to the school Online Safety Policy will be discussed in detail with all members of teaching staff and the Online Safety Group. The school will monitor the impact of the policy using:

- Logs of reported incidents
- Filtering
- Surveys / questionnaires of:
    - Pupils;
    - Parents / carers;
- Staff.

Appendices

- Student User Agreement Form : Acceptable Use Policy
- Key Stage 1 & Key Stage 2 Online Safety Pupil Agreements
- School Online Safety Curriculum MTP/ Resources
- School Safety Week Plans: showing Online Safety Content
- Incident Log Report Form: sample

Student User Agreement Form for the Student Acceptable Use Policy
(to form part of the Home/School agreement)

I agree to follow the school rules when using the school computers.

I will use the network in a sensible way and follow all the rules explained by my teacher.

I agree to report anyone not using the computers sensibly to my teacher.

I also agree to tell my teacher or another member of staff, if I see any websites that that make me feel unhappy or uncomfortable.

I will hand my mobile phone to the school office daily. (Year 5 & 6 only)

If I do not follow the rules, I understand that this may mean I might not be able to use the computers.

Student Name:

As the parent/legal guardian* of the pupil named above, I give permission for my child to access networked computer services such as the Internet and e-mail. I give permission for my child to bring their mobile phone to school. I understand that the mobile phone will be left in the school office during the school day.

I understand that pupils will be held accountable for their own actions.

I also understand that although the school will take reasonable steps to ensure that my child is appropriately supervised, according to age and responsibility, I will not hold the school or County Council responsible for inappropriate material that my child may obtain.

I understand the school reserves the right to apply monitoring arrangements to any student in relation to network, e-mail and Internet use where misuse is suspected. I accept responsibility for setting standards for my son or daughter to follow when selecting, sharing and exploring information and media. I agree to report any misuse of the network to the school.

Parent/Carer/Guardian's Name:

Parent/Carer/Guardian's Signature:

Date:

Key Stage 1 Online Safety Pupil Agreement

This is how I stay safe when I use computers or Ipads:

I will use the internet to help me learn.

I will only visit sites that my teacher has told me to use.

I will take care of the computer and other equipment.

I will ask for help from a teacher if I am not sure what to do.

I will tell a teacher 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 the computer.

Signed:.....

Key Stage 2 Online Safety Pupil Agreement

This is how I stay safe when I use computers or Ipads:

- I will use the internet to help me learn.
- I will only visit sites that my teacher has allowed me to use.
- I will use my own login and password.
- I will keep my password secret.
- I will not access other people's files.
- I will take care of the computer and other equipment.
- I will not copy, print, upload or download anything without my teacher's permission.
- In school I will only contact other people online with the permission of a teacher and when an adult is present.
- I will ask for help from a teacher if I am not sure what to do.
- I will tell a teacher if I see something that upsets me on the screen.
- I know that I can go to www.thinkuknow.co.uk for help.
-

I know that if I break the rules I might not be allowed to use the computer.

Signed:.....

Risby CEVC Primary School: **Online Safety Education. Resources**

EYFS	Childnet: Smartie the Penguin EYFS www.childnet.com/resources/smartie-the-penguin (EYFS ppt) - Smartie the Penguin - ebook Digiduck www.childnet.com/digiduck Digiduck e-book SWGFL Digital literacy www.digital-literacy.org.uk/ Lesson 1 Going Places Safely
Year 1	Childnet: Smartie the Penguin EYFS www.childnet.com/resources/smartie-the-penguin (Year 1 ppt) Thinkuknow: Hector's World www.thinkuknow.co.uk/teachers https://www.thinkuknow.co.uk/5_7/ (Hector's World) SWGFL Digital literacy www.digital-literacy.org.uk/ Lesson 2 ABC Searching Lesson 3 Keep it Private Lesson 4 My Creative Work
Year 2	Childnet: Smartie the Penguin EYFS www.childnet.com/resources/smartie-the-penguin (year 2 ppt) Thinkuknow: Lee & Kim www.thinkuknow.co.uk/teachers https://www.thinkuknow.co.uk/5_7/ (Lee & Kim) Skills School – Club Penguin Staying Safe http://www.childnet.com/young-people/primary/skills-school Australian Government: Comic Book Capers https://www.esafety.gov.au/comic-book-capers/ SWGFL Digital literacy www.digital-literacy.org.uk/ Lesson 1 Staying Safe Online Lesson 2 Follow the Digital Trail Lesson 3 Screen out the Mean Lesson 4 Using Keywords Lesson 5 Sites I Like
Year 3	Childnet: kara, Winston & the Smart Crew http://www.childnet.com/resources/the-adventures-of-kara-winston-and-the-smart-crew Thinkuknow: Hector's World www.thinkuknow.co.uk/teachers SWGFL Digital literacy www.digital-literacy.org.uk/ https://www.commonsensemedia.org/educators/scope-and-sequence Lesson 1 Powerful Passwords Lesson 2 My Online Community Lesson 3 Things for Sale Lesson 4 Show Respect Online Lesson 5 Writing Good Emails

Year 4	SWGFL Digital literacy www.digital-literacy.org.uk/ https://www.commonsensemedia.org/educators/scope-and-sequence Lesson 1 Rings of Responsibility Lesson 2 Private and Personal Information Lesson 3 The Power of Words Lesson 4 The Key to Keywords Lesson 5 Whose Is It, Anyway? Thinkuknow: Cyber Café and Play Like Share www.thinkuknow.co.uk/teachers https://www.thinkuknow.co.uk/8_10/
Year 5	Childnet: Only a Game (playscript) http://www.childnet.com/resources/only-a-game SWGFL Digital literacy www.digital-literacy.org.uk/ https://www.commonsensemedia.org/educators/scope-and-sequence Lesson 1 Strong Passwords Lesson 2 Digital Literacy Pledge Lesson 3 You've Won a Prize Lesson 4 How to Cite a Site Lesson 5 Picture Perfect Brain Pop Digital Etiquette https://www.brainpop.com/technology/digitalcitizenship/digitaletiquette/ Webwise : My Selfie https://www.webwise.ie/teachers/my-selfie/
Year 6	Childnet: Trust Me (Primary) http://www.childnet.com/resources/trust-me SWGFL Digital literacy www.digital-literacy.org.uk/ https://www.commonsensemedia.org/educators/scope-and-sequence Lesson 1 Talking Safety Online Lesson 2 Super Digital Citizen Lesson 3 Privacy Rules Lesson 4 What's Cyberbullying? Lesson 5 Selling Stereotypes BBC Horrible Histories : Saxon Monk – Internet Videos are Forever http://www.bbc.co.uk/cbbc/watch/p01g2pg0 Guy Fawkes – Protect Thy Privacy Settings http://www.bbc.co.uk/cbbc/watch/p01g2pt6 Lady Jane Grey – Beware What You Download http://www.bbc.co.uk/cbbc/watch/p01g2ppl Prudish Victorian – What happens when you lie about your age online? http://www.bbc.co.uk/cbbc/watch/p00nxznx Media Smart : Advertising and Body Image http://mediasmart.uk.com/resources/teaching-resources/body-image Thinkuknow: Jigsaw www.thinkuknow.co.uk/teachers

School Safety Week: Showing Online Safety Content

Year A	EYFS	Y1/2	Y3/4	Y5/6
Monday	Keeping Healthy – Sports Day			
Tuesday Out and About	Sun Safety, Crossing the Road, Out & about- holding an adults hand. Animals- dogs.	Road Safety- THINK role play. Water Safety- Staying safe on the beach.	Road Safety- THINK Safe places to cross. In Cars-car Seats & seat belts Water Safety- red flag, inflatables. Getting help.	Road Safety- THINK Cycle/,skate safety. Safety gear-helmets, hi-vis,, safe places to go. Water Safety Tides, currents ,lakes, ponds, rivers, canals. Water rescue- In trouble - what to do, how to help.
Wednesday Staying Safe Inside	Staying safe at Home m:edicines, chemicals, knives, hot things etc. Staying Safe at School Being kind, scissors, strangers in school, fire drill/alarm. My Body- my bubble, personal space,	Preventing Accidents Medicines, chemicals Electricity-sockets Fire- drop & roll Fire drill at school. Trip hazards.	Preventing Accidents Fire- matches, candles drop & roll. Electricity- spotting hazards at home Risk awareness- knives, rocking on chairs, stairs, door hinges etc.	Preventing Accidents Fire- matches , candles, smoke alarms, escape plans. Gas- leaks. Carbon Monoxide Drugs , medicines alcohol, smoking.
Thursday Healthy Me	Healthy Food-Trying different fruit & veg. Mental Health Recognising Emotions Self Esteem Relaxation	Healthy Eating Healthy Snacks and Drinks-food swaps	Healthy Eating Food Groups-Balanced Plate, Food Pyramid Hydration-drinking water	Healthy Eating Food Hygiene-Micro organisms Body Image
Friday Getting Help	People Who Help Us	People Who Help Us At school- Who can I talk to? Who can I tell ? Problem solving. Meet my MDSA.	People Who Help Us Bullying- Coping with problems Who Can I talk to ? Meet my MDSA	People Who Help Us Who Can I talk to ? Getting help- NSPCC,Childline etc Reporting Abuse Online Meet my MDSA

Year B	EYFS	Y1/2	Y3/4	Y5/6
Monday	Keeping Healthy – Sports Day			
Tuesday Out and About	Sun Safety. hat, sun cream. Crossing the Road, Out & about- holding an adults hand. Plants, berries Animals- dogs.	Sun Safety hat, sun cream, water Playing Safely safe places to play plants, berries Stranger Danger Animals –dogs.	Sun Safety hat, sun cream, water, time in sun. Playing Safely safe places to play trampolines, Risk assessment, dangers of building sites, railway lines, roads, tree climbing. finding thing-syringes. Plants & Animals-bees, wasps.	Sun Safety hat, sun cream, water, time in sun SPF, UV, tanning dangers and alternatives Playing Safely Animals- cows, bulls, swans, horses, adders, ticks Lyme Disease. Walking home, being out alone., telling an adult where you are going & time home. Shopping Safely- keeping purse, phone safe. Shoplifting …what to do.
Wednesday Staying Safe Inside	Staying safe at Home m:edicines, chemicals, knives hot things etc. At School-Being kind, scissors, strangers in school,fire drill/alarm. My Body- my bubble,	My Body- Personal space, safe touches, respecting each other.	Screen safe Age appropriate- PEGI ratings, cinema ratings TV programmes, dvd, video games. Hours online, playing video games. Safe playing online.	Respect- relationships…your body your choice. Chat rooms, webcams, social media, safe surfing, uploading, blogging, vlogging.
Thursday Healthy Me	Healthy Food-Trying different fruit & veg. Recognising Emotions Self Esteem Relaxation	Mental Health Self Esteem Anger Management Relaxation	Mental Health Self Esteem Managing Conflict Dealing with Worries Relaxation	Mental Health Managing Change Coping with Stress Self Esteem- body image, social media validation(likes). Relaxation
Friday Getting Help	People Who Help Us	People Who Help Us Calling 999-role play Police Getting Lost- what to do Safe Adults	People Who Help Us Doctors and Dentists Tooth care	First Aid

Incident Log Report Form

Reporting Log

Group: .....

Date	Time	Incident	Action Taken		Incident Reported By	Signature
			What?	By Whom?		