Online Safety Policy

Updated:	February 2018
By:	Mr P Kennedy
Approved by Governors:	
The Deputy Headteacher is responsible for monitoring this policy.	
Signature of Chair of Governors Date:	
Signature of Head teacher Date:	
Date of next review:	February 2019

Contents

1.	Introduction	3
2.	St. Charles R. C. Primary School's Vision for Online Safety	4
3.	Online Safety Lead	4
4.	Security and data management	5
5.	Use of mobile devices	5
5a.	Mobile phones	5
5b.	Other mobile devices	6
6.	Use of digital media (cameras and recording devices)	6
7.	Communication technologies	8
7a.	Email	8
7b.	Social Networks	9
7c.	Instant Messaging or VOIP	9
7d.	Virtual Learning Environment (VLE)	10
7e.	Websites and other publications	10
8.	Infrastructure and technology	10
8a.	Children's access	10
8b.	Adult access	11
8c.	Passwords	11
8d.	Software/hardware	11
8e.	Managing the network and technical support	11
8f.	Filtering and virus protection	12
9.	Dealing with incidents	12
9a.	Illegal offences	13
9b.	Inappropriate use	13
10.	Acceptable Use Policy (AUP)	13
11.	Education and training	14
11a.	Online Safety – Across the curriculum	15
11b.	Online Safety – Raising staff awareness	15
11c.	Online Safety – Raising parents/carers awareness	16
11d.	Online Safety – Raising Governors' awareness	16
12.	Evaluating the impact of the Online Safety Policy	16
	Appendices	

1. Introduction

Online Safety encompasses internet technologies and electronic communications, such as mobile phones, as well as collaboration tools and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

The potential that technology has to impact on everyone increases year on year. This is probably even more true for children, who are generally much more open to developing technologies than many adults. In many areas, technology is transforming the way that schools teach and that children learn. At home, technology is changing the way children live and the activities in which they choose to partake; these trends are set to continue.

While developing technology brings many opportunities, it also brings risk and potential dangers of which these are just a few:

- Access to illegal, harmful or inappropriate images or other content;
- Unauthorized access to/loss of/sharing of personal information;
- The risk of being subject to grooming by those with whom they make contact with on the internet;
- The sharing/distribution of personal images without an individual's consent or knowledge;
- Inappropriate communication/contact with others, including strangers;
- Cyber-bullying;
- Access to unsuitable video/internet games;
- An inability to evaluate the quality, accuracy and relevance of information on the internet;
- Plagiarism and copyright infringement;
- Opportunities to encounter racial hatred and extremism;
- Illegal downloading of music or video files; and
- The potential for excessive use which may impact on social and emotional development and learning.

This policy sets out how we strive to keep children safe with technology while they are in school. We recognise that children are often more at risk when using technology at home (where we have no control over the technical structures put in place to keep them safe) and so this policy also sets out how we educate children of the potential risks. We also explain how we attempt to inform those people who work with our children beyond the school environment (parents, friends and the wider community) to be aware and to assist in this process.

This policy was created in accordance with the Lancashire Online Safety Policy Guidance Document. It reflects the needs of St. Charles and will be updated on an annual basis or before, if there is a change in circumstances, new equipment or incidents within school. This policy will be shared with the whole community at St. Charles and will be used in conjunction with other policies, including Safeguarding, Behaviour and Data Protection.

2. St. Charles R. C. Primary School's Vision for Online Safety

St. Charles R. C. Primary School aims to provide a safe and secure environment, which not only protects all people on the premises but also educates them on how to stay safe in the wider world.

This will include:

- learning about the safe use of new technologies;
- recognising and managing the potential risks associated with online activities;
- behaving responsibly online;
- recognising when pressures from others in the online environment might threaten their personal safety and well-being;
- developing effective ways of resisting pressure
- knowing who to go to with any concerns.

3. Online Safety Lead

The Online Safety Lead at St. Charles is Mr. Kennedy and he is the main point of contact for any Online Safety related issue and incident. He is also a DSL.

The Online Safety Lead's role includes:

- Having operational responsibility for ensuring the development, maintenance and review of the school's Online Safety Policy and associated documents, including the Acceptable Use Policy;
- Ensuring that the policy is implemented and that compliance with the policy is actively monitored;
- Ensuring all staff are aware of reporting procedures and requirements should an Online Safety incident occur;
- Ensuring an Online Safety Incident Log is appropriately maintained and regularly reviewed;
- Keeping personally up-to-date with Online Safety issues and guidance through liaison with the Local Authority and through advice given by national agencies, such as the Child Exploitation and Online Protection Centre (CEOP);
- Providing and arranging Online Safety advice/training for staff, parents/carers and Governors;
- Ensuring the Head teacher, SLT, staff, children and Governors are updated as necessary;
- Leading the Online Safety Group to ensure that it monitors the Online Safety provision effectively within school and holds the Online Safety Lead to account.
- Liaising closely with the school's main Designated Senior Lead to ensure a coordinated approach across relevant safeguarding areas.

4. Security and Data management

In line with the requirements of the Data Protection Act (1998), sensitive or personal data is recorded, processed, transferred and made available for access in school.

The school has a Data Protection Policy which covers all aspects of Security and data management. This is currently being updated to fall in line with the new requirements around Data Protection (GDPR) which comes into effect in May 2018.

5. Use of mobile devices

THE INAPPROPRIATE USE OF ANY MOBILE DEVICE WHILST ON SCHOOL PREMISES IS NOT ACCEPTABLE. ANYBODY SEEN USING A DEVICE INAPPROPRIATELY WILL BE CHALLENGED AND REPORTED TO THE HEAD TEACHER OR ONLINE SAFETY LEAD

Inappropriate use includes:

- The use of mobile devices in toilets and changing areas.
- The recording of images, video and audio on a personal device without prior approval from the Head teacher or Deputy Head teacher, apart from events such as Sports Day, Christmas and fundraising events which may be recorded by parent/carers but always in full view of all attending.

The incident/escalation procedures and sanctions for inappropriate use can be found in Appendix 1.

The school cannot be held liable for any damage or theft of personal devices.

Mobile Phones

Staff

- All members of school staff are allowed to use their personal mobile phones on the premises for their own personal use.
- When working directly with children, staff are not to have their mobile phones on their person.
- Staff are asked not to make personal calls/messages during their working hours. However, in urgent cases a call may be made or accepted if deemed necessary and by prior arrangement with the Head teacher. The school office can also be used as a point of contact in the event of an emergency.
- All mobile phones must be placed 'on silent' mode or turned off during working hours.
- The security of personal mobile phones is the responsibility of the owner.
- The use of the school's Wi-Fi connection for access to the internet is permitted.
- If personal mobile phones are automatically synced to access work related e-mails, they must be password protected.

Children

- If a child requires a mobile phone for emergency contact purposes before and/or after school, then it should be handed into the school office at the beginning of the day and

collected at the end. An agreement form must be signed in advance of this: Mobile Phone Procedure for Pupils
- The school office is the point of contact for any child in the event of an emergency.
- Staff are empowered to confiscate a mobile phone if it has not been handed into the school office at the beginning of the day and they believe it is being used to contravene this policy or the school's safeguarding, behaviour or bullying policies.

School
- The school has a mobile phone for the After School Club. The After School Club manager is responsible for its use.
- The school mobile phone can be used by all school staff as a point of contact whilst on educational visits. The After School Club manager is responsible for ensuring the device is fully charged and ready for use.

Visitors
- Visitors are reminded upon entry to the school by the office staff to place their mobile phone onto silent and not to use it when around children.
- Staff are to be vigilant and monitor visitors for any covert use of mobile phones.

Other mobile devices
- The use of other mobile devices in school are risk assessed and balanced against their potential benefits for learning.
- No personal mobile devices are to be used in school unless expressed approval has been sought and approved by the Head teacher or the Deputy Head teacher.
- It is the responsibility of the device owner to ensure all content on the device is legal and appropriate for a school setting.
- The school has a class set of iPod touches and 42 iPads which are to be used in conjunction with the curriculum. They are also used outside of school to record images and videos during educational visits.
- The use of SMART watches with video/camera functionality is not allowed.

6. Use of digital media (cameras and recording devices)

Consent and Purpose

Written consent for the use of digital media is sought when a child joins St. Charles. The consent form details the different ways that the school may use a child's image, these are:
- Use in our printed publications;
- Displays around school;
- As teaching resources for use within the curriculum;
- On the school website, Twitter, Facebook and ClassDojo!
- Use by school approved 3rd parties, e.g. local newspaper/television

Video clips may also be used:
- As teaching aids within the curriculum;

- For staff training;
- For educational purposes at both local and national level.

Where a trainee, not directly employed by the school, would like to use children's images in portfolios of work, parental permission must be sought on an individual basis.

As digital media evolves and adapts it may be appropriate for the school to update digital media consent forms to include new technologies. Where possible, images of children who have left the school will be deleted during the course of the next school year.

Taking Photographs/Video

All staff employed by the school are authorised to take photographs/video clips and are reminded to check consent forms before their publication. Staff iPods/iPads are used to take photographs/video clips and may only use their own personal devices once the expressed permission of the Head teacher or Deputy Head teacher is given. These images/video clips must be deleted from personal devices once they have been published.

The rights of an individual to refuse to be photographed will be respected. Images/video clips of children who are distressed, injured or in a context that could be embarrassing or misinterpreted will not be taken or published. The context for all photographs/video clips will be assessed and deemed appropriate for use. Close up shots are avoided. Pictures will preferably include a background context and show children in group situations.

Parents Taking Photographs/Videos

Under the Data Protection Act (1998), parents are entitled to take photographs/video clips of ***their own*** children on the provision that they are for ***their own*** use, e.g., events such as Sports Day, Christmas and fundraising events. **The inclusion of other children or use of images/video clips for other purposes could constitute a potential breach of Data Protection legislation.**

Parents are informed of their entitlement through the school's newsletter ahead of an event. They are also made aware that publishing images which include children other than their own or other adults on Social Network sites is not acceptable, unless specific permission has been obtained from the individuals' parents. Consideration of others is encouraged when taking photographs so as not to obscure an individual's view or being intrusive.

Storage of Images/Videos

Photographs and videos that are taken on staff iPods/iPads are automatically stored securely in school on the 'P Drive'. This device is a secure server in school. Images and video clips stored on school devices are removed on a half-termly basis and added to the school's secure password protected server. All staff have password protected USB devices for the transfer of images from one device to another.
The storage and transferring of images and videos on personal devices is the responsibility of the owner. As mentioned previously, expressed permission needs to be sought from the

Head teacher or Deputy Head teacher beforehand. If permission is granted, staff will be reminded to erase images as soon as they have been published.

Publication of Images/Videos

Consent has been obtained for the publication of children's images in displays, school publications, teaching resources and on the school website, Facebook and Twitter. When publishing photographs, care is taken over the choice of images used so that images cannot be made available for downloading or misuse, e.g. through the use of low definition images that will not magnify effectively. Only first names will be added to pictures. Other personal information will not accompany published images.

3rd Parties and Copyright

3rd parties are supervised at all times whilst in the school and every effort is made to ensure they comply with the Data Protection requirements in terms of taking, storage and transfer of images. The copyright for images taken by a 3rd party are retained by the 3rd party.

By consenting to 3rd parties taking photographs, parents/carers are bound by the terms and conditions of the 3rd party. This means that the 3rd party may modify, copy or redistribute the images without further consent.

CCTV, Video Conferencing, VOIP and Webcams

CCTV cameras are used to monitor the outdoor environment of the school. These cameras record 24/7 to ensure the building is kept safe. Access to the recordings is restricted to the Head teacher, Deputy Head teacher and the Office Manager.

The use of Video Conferencing, VOIP (Voice-over-Internet Protocol) and Webcams are in use within school. These facilities have been used through 3rd party providers, e.g. National Archives session provided through v-scene.

7. Communication technologies

Email

All staff have access to the Microsoft 365 email system. It is the responsibility of these staff members to ensure that the content of all school emails is kept secure and remains confidential. Emails are used to transmit important information to all members of the school community on a daily basis. Staff are reminded on a regular basis of their responsibility to maintain professional use of the email system. They are also prompted to change their password every 3 months.

Each class has access to an e-mail account. The password for this account is kept by the class teacher in order to monitor the account for appropriate use.

As part of the school curriculum, staff and children are educated as to the dangers of accessing content including SPAM, phishing, unsuitable materials and viruses from external email accounts, e.g. Hotmail or Gmail, in school. They are also made aware that the use of email is covered by The Data Protection Act (1998) and the Freedom of Information Act (2000) which means that safe practice should be followed in respect of record keeping and security. Finally, they are taught not to open attachments that they suspect may contain illegal content as they could inadvertently be committing a criminal offence.

Any email received that makes users feel uncomfortable, is offensive, threatening or bullying nature should be referred to the Online Safety Lead.

All staff are advised to add the following disclaimer at the bottom of all outgoing email communications.

This e-mail and any files transmitted within it may be confidential and are intended solely for the individual to whom it is addressed. Any views or opinions presented are those of the author and do not necessarily represent St Charles' RC Primary School. If you are not the intended recipient, you must not use, disseminate, forward, print or copy this e-mail or its contents. If you have received this e-mail in error, please contact the sender. Please note that e-mail may be monitored in accordance with both school policy and the Telecommunications (Lawful Business Practices) (Interception of Communications) Regulations 2000.

Social Networks

The school uses 2 social networking sites (Facebook and ClassDojo!). All are used as a means of communicating to parents and to gain feedback on different events within school. They are managed by the Head teacher and Deputy Head teacher. It is their responsibility to ensure the content of these sites is appropriate and complies with school policies. Any content posted on these sites by 3rd parties deemed inappropriate will be removed at the earliest opportunity and their access to the site blocked.

Parents and children have access to the ClassDojo! site. Information (in the form of messages and photos) can be instantly communicated to parents. Access to this site is policed by the class teacher and overseen by the Online Safety Lead. The school office have access in order to send messages to parents where necessary. Any communication received by a class teacher deemed inappropriate or offensive is to be referred to the Online Safety Lead or Head teacher.

Personal use of Social Networking sites by school staff is addressed in the 'Social Media Policy'.

Virtual Learning Environment (VLE) – Purple Mash

The school's VLE is managed by the Online Safety Lead and his role on the site is Administrator. It is his responsibility to ensure that all information stored in the VLE is accurate and does not contain inappropriate content. All staff are given the role of Teacher and pupils are enrolled with Student responsibilities. Passwords are issued during

enrolment. Once staff and children leave the school it is the responsibility of the Administrator to delete their accounts.

Website and other online publications

The school website is the main way the school will communicate Online Safety messages to parents/carers. There is a dedicated Online Safety section of the site which contains up to date information on developments and publications.

All staff have access to the school website and it is their responsibility to ensure they follow the school's policy for the publication of digital media and personal information on the site. Downloadable materials on the website are published in PDF format where necessary to prevent content being manipulated and potentially re-distributed without the school's consent.

The Online Safety Lead assumes overall responsibility for what appears on the school website.

8. Infrastructure and technology

The school subscribes to the Lancashire Grid for Learning and the BTLS Broadband Service (internet content filtering is provided by default through this service). The filtering service offers a high level of protection but occasionally unsuitable content may get past the filter service. The school has the ability to allow access to certain restricted websites. This has to be approved by the Head teacher. Current websites allowed can be found in Appendix 2.

Children's access

Children are supervised at all times, including break times, lunchtimes and during After School Clubs when accessing school equipment and online materials. There will always be a member of staff present in the room when the children are online. When using an iPad or iPod there is no individual or class log-ins.

If children come across unsuitable material, they are instructed to close the lid of a MacBook or turn off an iPad/iPod and report it to the nearest member of staff.

Adult access

Adults in the school have the same filtered access to the internet as the children. It is the responsibility of all adults to monitor the internet use of all children in their care. Any websites reported or discovered during the planning and delivery of lessons are to be reported to the Online Safety Lead who will then report the website details to the Lancashire Grid for Learning filtering service via the e-mail address block@ict.lancsngfl.ac.uk

Passwords

Staff laptops and MacBooks are password protected. The password on Staff MacBooks is shared with all adults employed within the school so they can access and use the Promethean teaching resources installed on them. The password on staff laptops and is personal to them and adheres to the security measures set out in the school's Password Policy. iPads and iPods provided for the children are not password protected for log-in but there are secure areas password protected which ensure the system settings are maintained. The password to access these settings is known by the Online Safety Lead, Head Teacher and the school's technical support providers, Nybble.

Staff and children are reminded on a regular basis to keep passwords secure. There is no set timescale for the changing of passwords. Passwords on staff MacBooks, system settings and the wireless network are set to a mixture of letters and numbers.

Software/hardware

All software and hardware in school has been purchased by the school and the school has legal ownership of it. There is a record of appropriate licenses for all software. It is the responsibility of the school office to ensure this is updated on an annual basis and shared with all stakeholders.

Managing the network and technical support

All servers, wireless systems and cabling are securely located and physical access is restricted. Wireless devices have had security settings put in place to protect them. Access to the internet is restricted through Local Area Network proxy settings and a secure password is in place.

iPod touch devices in school have had access settings put in place to restrict the access to and downloading of restricted content, the downloading of apps, 'in-app' purchases and the changing of settings.

The management, safety and security of the school's network has been delegated to Nybble Information Systems. The safety and security of the network is reviewed on an on-going basis. It is their responsibility to ensure the school systems are kept up to date in terms of security.

School MacBooks, iPads and iPods are kept up to date by the Online Safety Lead. The installing of software and downloading of executable files on shared devices is the responsibility of the Online Safety Lead.

Any suspicion or evidence of a breach of security needs to be reported to the Online Safety Lead at once, or the Head teacher if not available.

Class teachers have been issued with password encrypted removable storage devices for the transferring of sensitive information. The use of staff laptops, MacBooks and iPads at home is permitted so long as the necessary precautions are taken to ensure any sensitive information contained within is password protected.

Any network monitoring taking place is done in accordance with the Data Protection Act (1998) and all staff will be made aware of any network monitoring that takes place and by whom.

This document will be shared with all internal/external technical support providers to ensure they are abiding by the school's Online Safety policy. It is the responsibility of the Online Safety Lead to do this.

Filtering and virus protection

The school has some devolved control of the Lancashire Grid for Learning filtering service. Any websites filtered by Lancashire that have been approved by the school are listed in Appendix 2.

The filtering is managed and approved by the Head teacher. The list of approved websites can be found in Appendix 2 of this document. Any new websites the school has allowed are shared with staff during staff meetings.

Staff are aware of the procedures for blocking (report to Online Safety Lead) and unblocking (request to the Head teacher) specific websites.

It is the responsibility of staff to ensure their laptops have sufficient virus protection installed. Sophos is automatically installed on all school laptops. Any computer virus infection detected on a laptop is to be reported to the Online Safety Lead who will then assess and refer to Nybble if required.

9. Dealing with incidents

An incident log is in place and is completed to record and monitor offences. This is audited on a half-termly basis by members of the Senior Leadership Team. It is essential that correct procedures are followed when responding to an Online Safety incident to ensure escalation procedures are followed accordingly and any evidence is preserved to protect those investigating the incident.

Illegal offences

Any suspected illegal material or activity must be brought to the immediate attention of the Head teacher and Online Safety Lead. They will then refer it to external authorities, e.g. Police, CEOP, Internet Watch Foundation (IWF). The Head teacher, Online Safety Lead or any other member of school staff will never personally investigate, interfere with or share evidence as this may inadvertently be committing an illegal offence. Any potentially illegal content will always be reported to the IWF as they are licensed to investigate.

Examples of illegal offences are:

- Accessing child sexual abuse images;
- Accessing non-photographic child sexual abuse images;

- Accessing criminally obscene adult content;
- Incitement to racial hatred.

Inappropriate use

Any Online Safety incidents which involve inappropriate use will initially be referred to the Online Safety Lead. He will then investigate the incident and, if appropriate, use the Sanctions guide (Appendix 1) as a reference for disciplinary procedures. Any offence committed which is not contained within this guide will be referred to the Online Safety committee (Online Safety Lead, Head teacher and Chair of Governors) to decide upon appropriate disciplinary procedures.

The Sanctions Guide has been issued to all members of the school staff as a reference guide and it has also been made available to all children and parents via the school website. The sanctions guide also details the incidents where parents or external agencies will become involved. Incidents are logged with the Online Safety Lead who then shares the log with the SLT on a half-termly basis.

Where possible, measures will be put in place to prevent recurrence of an incident and training for children put in place too.

Where there is a suspected incident/allegation involving a member of staff, this is to be confidentially reported to the Online Safety Lead or Head teacher who will then discuss this issue with other members of the Online Safety committee and devise a plan of action. The confidentiality of the whistle-blower will be maintained at all times.

Inappropriate use also includes bringing into school banned items, including electronic devices. As stated in our Behaviour Policy under the Education Act (2011), school has the power to 'search' any pupil suspected of bringing into school a banned device. Sanctions will be in line with the guide in Appendix 1.

10. Acceptable Use Policy (AUP)

An AUP is intended to ensure that all users of technology within school are responsible and are protected from potential risk in their everyday use of ICT for educational, personal and recreational purposes.

AUPs are read, signed and adhered to by all staff, children and visitors before access to technology is allowed. An AUP is a partnership between parents/carers, children and the school to ensure that users are kept safe when using technology. A list of children who are not allowed to access technology is kept in the school office and made available to staff. It is shared by the Online Safety Lead as and when required.

Copies of the school's AUPs can be found in Appendices 4, 5 and 6.

11. Education and training

In 21st Century society, both adults and children need to be digitally literate and aware of the benefits that the use of technology can provide. However, it is essential that children are taught to use technology responsibly, securely and safely by being able to recognise potential risks and know how to respond. They should, for example, be able to communicate safely and respectfully online, be aware of the necessity to keep personal information private, be taught how to search effectively, be discerning in their evaluation of digital content and be aware of the need to respect copyright and Intellectual Property rights.

OFSTED highlight three main areas of Online Safety risk which all members of staff are aware of and incorporate into the ICT curriculum at every opportunity. These areas are:

- Content – children need to be taught that not all content is appropriate or form a reliable source
    - Exposure to inappropriate content, including online pornography, ignoring age ratings in games (exposure to violence associated with often racist language), substance abuse.
    - Lifestyle websites, for example pro-anorexia/self-harm/suicide sites
    - Hate sits.
    - Content validation: how to check authenticity and accuracy of online content.
- Contact – children need to be taught that contact may be made using digital technologies and that appropriate conduct is necessary when engaging with these technologies
    - Grooming
    - Cyberbullying in all forms
    - Identify theft (including 'frape' – hacking Facebook profiles) and sharing passwords.
- Conduct – children need to be made aware that their personal online behaviour can increase the likelihood of, or cause harm to themselves and others.
    - 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).
    - Copyright (little care or consideration for intellectual property and ownership – such as music and film).

Online Safety – Across the curriculum

It is vital that children are taught how to stay safe, protect themselves from harm and take a responsible approach to their own and others' Online Safety.

At St. Charles we aim to provide relevant, flexible and engaging Online Safety education to all children as part of their curriculum entitlement. In order to do this we address the following points.

- As part of the computing curriculum, there is regular, planned Online Safety teaching within a range of curriculum areas. These incorporate the Lancashire ICT Progression document guidance on Online Safety contained within the Electronic Communication

and Digital Research sections. Children are taught to critically evaluate materials and develop good research skills through cross-curricular teaching and discussions. Older children are taught about the relevant legislation when using the internet, e.g. Data Protection Act (1998) and copyright implications.

- To ensure Online Safety education is progressive throughout the school, the Online Safety Lead and Computing Lead is the same person and has created a whole school progression document. This will be made available to all stakeholders.
- As with all teaching at St. Charles, Online Safety education will be differentiated to meet the needs of all pupils.
- The school has an additional focus on Online Safety during Safer Internet Day.
- During Anti-Bullying week, the impact of cyberbullying is highlighted and children are reminded of how to seek help if they are affected by these issues. The use of 'Whisper' technology is in use on the school website.
- The AUP is shared with children and sections highlighted throughout the year. This is to encourage safe and responsible use of ICT both within and outside of school.
- When using electronic devices, children are reminded of safe internet use.

Online Safety – Raising staff awareness

Staff audits are carried out every year to ascertain the level of knowledge and expertise in the use of new technologies and their potential benefits and risks. From this audit, staff Online Safety training is carried out. Training is delivered by the Online Safety Lead who will then monitor the impact. The Online Safety Lead will be the point of contact for any advice/guidance as and when required.

Staff are made aware of issues which may affect their own personal safeguarding, e.g. use of Social Network sites, through the school's Social Media Policy. Any concerns should be raised with the Online Safety Lead or the Head teacher.

Staff are expected to promote and model responsible use of ICT and digital resources. All staff have agreed to this upon signing the AUP.

As part of the induction programme for all new staff, Online Safety training is provided to ensure a full understanding of the school's Online Safety policy and AUP.

Regular updates on Online Safety are discussed at staff meetings as and when required.

Online Safety – Raising parents/carers awareness

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

In order to support parents/carers, the school is looking to provide regular updates to support and develop their understanding. This will help to keep them informed about Online Safety, including the benefits and risks of using various technologies, both older and new, and at home and at school. In order to do this, the school will provide:

- Regular updates through the school newsletter;
- Share relevant aspects of the school's Online Safety Policy

- Distribute resources received in school;
- Provide links through the Online Safety section of the school website;
- Deliver Bespoke Parents Online Safety Awareness sessions;
- Promote external Online Safety resources/online materials.

Online Safety – Raising Governors' awareness

The Online Safety Lead will be the main point of contact for Governors whose responsibilities fall under the remit of Online Safety, e.g. ICT or child protection. It is the responsibility of the Online Safety Lead to communicate relevant information to ensure Governors are up to date.

12. Evaluating the impact of the Online Safety Policy

The Online Safety Policy is to be reviewed in February 2019. As part of this review process, the Online Safety Lead will talk to all stakeholders to discuss the impact of the policy and whether it is addressing relevant issues regarding Online Safety. New technologies with be assessed and amendments made to the school's Online Safety Policy if required.

Every half-term the SLT will review the incident log and analyse incidents to see if there are any recurring patterns and, if so, how these can be addressed most effectively. Upon reviewing the incidents, it will then be decided by the SLT whether these incidents require changes to be made to the Online Safety policy and school practices. It will then be decided how to inform stakeholders of these changes.

AUPs will be reviewed on an annual basis and, where possible, changes made to address current trends and new technologies. Only when changes are made will new copies be sent home to be signed. Parents will be reminded of the AUPs at regular intervals during the school year and copies can be found online.