Holy Family Catholic Primary School

e-Safety Policy

This e-Safety Policy has been written as part of a consultation process involving the following people:

(number) Staff members, (number) Governors, Parents who attended our recent e-Safety session conducted by Name & pupils.

It has been approved by Governors and will be monitored and reviewed as listed below:

Policy Created - Date: Sept 2018

Policy Review - Date: October 2018. (Standards & Effectiveness Committee)

Next Review October 2019

The implementation of this policy will be monitored by: HT, DSL, DHT & e-safety governors. This policy will be reviewed as appropriate by: HT, DSL, DHT & e-safety governors and all staff

Reviewed & Approved by J.Westray (Headteacher)

Date: 30th September 2018

Reviewed & Approved by (Name) on behalf of S & E committee (Governor)

Date: ___ October 2018

Contents

INTRODUCTION

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

OUR SCHOOL VISION FOR E-SAFETY

Holy Family Catholic Primary School provides a diverse, balanced and relevant approach to the use of technology. Children are encouraged to maximise the benefits and opportunities that technology has to offer. We ensure that children learn in an environment where security measures are balanced appropriately with the need to learn effectively.

Children are equipped with the skills and knowledge to use technology appropriately and responsibly. At our school we teach how to recognise the risks associated with technology and how to deal with them, both within and outside the school environment. All users in our school community understand why there is a need for an e-Safety Policy.

3. The school’s e-Safety Champion

Our school e-Safety Champion is Steve Barlow who is a member of our SLT. The e-Safety Champion is the main point of contact for e-Safety related issues and incidents. The role of the e-Safety Champion includes:

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

4. Security and data management

ICT security is a complex subject that involves all technology users in the school, dealing with issues regarding the collection and storage of data through to the physical security of equipment. In line with Lancashire ICT Security Framework (published 2005) procedures are in place to ensure data, in its many forms, is kept secure within the school, in line with the requirements of the Data Protection Act (1998), sensitive or personal data is recorded, processed, transferred and made available for access in school.

This data must be:

- Accurate.
- Secure.
- Fairly and lawfully processed.
- Processed for limited purposes.
- Processed in accordance with the data subject’s rights.
- Adequate, relevant and not excessive.
- Kept no longer than is necessary.
- Only transferred to others with adequate protection.
- All data in school must be kept secure and staff informed of what they can or can’t do with data through the e-Safety Policy and statements in the Acceptable Use Policy(AUP).

Does your school map key information that is held?

Information is held in various ways; on SIMS, Data Sheets, Pupil contacts, SEN & Referrals. All this information is kept securely at all times & if taken off site must be recorded with e-Safety champion /HT/business manager & continued to be secure at all time.

Is there a named person with responsibility for managing information?

The Headteacher, Janet Westray, is responsible in our school.

Do relevant staff know the locations of data?

All relevant staff are aware of the locations of data.

Do all staff with access to personal data understand their legal responsibilities?

All staff with access to personal data know and understand the importance of their legal responsibilities regarding data protection. Reminder of responsibilities undertaken Oct 2017 with staff

How will your school ensure that data is appropriately managed both within and outside the school environment?

Data will be managed, recorded, registered & monitored by the Headteacher/Business Manager

Are staff aware that they should only use approved means to access, store and dispose of confidential data?

All staff are aware that confidential data should be shredded & disposed of correctly. All staff are aware that and devices for storing data should be encrypted or password protected.

If staff have remote access to school data, how do you ensure the data remains secure, e.g. are staff aware of the dangers of unsecured wireless access at home?

Staff who use remote access have set up computers in line with guidelines & do not use unsecured wireless at any time.

Do you allow the use of 'cloud' storage facilities e.g. Dropbox / SkyDrive or external storage related to software used for creation of children's profiles (especially in Early Years)?

Yes but no personal information about children /photos should be uploaded to a cloud facility at any time.

How do you ensure that data is securely stored and satisfies the requirements of the Data Protection Act?

Anyone with access to personal data must ensure PC is password protected as all computers in school are. Must log-off when computer is left.

What is your school's policy on using mobile devices and removable media?

Is this allowed and if so: how Is data on these devices password protected and encrypted? These devices may be used but must be password protected & encrypted.

Are the devices themselves password protected and encrypted?

Yes

Are devices containing data allowed to be removed from the school premises?

No

How does your school ensure personal devices are not used to access data on school systems e.g. downloading e-mail or files to a Smartphone?

Staff are aware this is not allowed and are also aware the headteacher may check school systems for misuse.

How does your school ensure the risk of data loss is addressed and managed?

Staff must follow guidelines in this policy and sign the A.U.P. on an annual basis.

What is your school's procedure for backing up data?

The school server is backed up through our internet provider Virtue Technologies. The admin computer is backed up externally by BT Lancashire.

5. Use of mobile devices

School use of mobile devices, including laptops, tablets, mobile phones, cameras and games consoles is becoming more commonplace. Whilst these can provide a flexible solution and offer a range of exciting opportunities to extend children's learning, their use poses challenges in terms of e-Safety. Many of these devices integrate functionality to take images, access the Internet and engage users in various methods of external communication. At Holy Family Catholic Primary School devices e.g. iPads/notebooks are provided for use in class, Children are not allowed to bring their own devices into school.

Areas discussed:

Do you allow use of personal mobile phones by adults or children in school?

Children are NOT allowed mobile phones in schools and these will have to be held in the office until the end of the day. Adults may use mobile phones in their own time but only in the staff room area or their own cars. They can use their mobiles phones to logon to secure systems like CPOMS within classrooms.

Do you have designated 'mobile phone free' area(s) where the use of phones is not allowed e.g. toilets or changing areas?

No mobile phone should be used in toilets/cloakrooms

Do you have designated times when use of personal mobile phones is allowed e.g. lunch or break times?

Staff may use mobile phones at break time & lunch time in appropriate areas away from children.

Do you require mobile phones to be switched off or 'on silent' during the school day?

Yes

Is there a safe and secure area where personal mobile phones can be stored when not in use e.g. lockers for adults or a requirement for children to take mobile phones to the office for safe storage?
Staff must ensure phones are in a safe, secure area and children must take phones to the office.

Are personal mobile phones expected to be security marked, password protected and insured?

This is the individual member of staff's responsibility.

How can children, staff or visitors be contacted in the event of an emergency?

Contacts are held on SIMS, in the contact file & loaded onto our texting service. Admin staff will pass on any messages or will inform the person that there is a call.

Do you have very clear statements to say that images, video or audio must not be recorded on a personal mobile phone without specific authorisation from the headteacher?

Only with authority from the headteacher and must be deleted once loaded onto secure school server and made available for HT to examine.

Do you allow users to access the Internet via personal mobile phones using the school's wi fi connection (if available)? Only for work base systems like CPOMS

Do you have a 'work' device for staff to use, for example, whilst outside the main buildings or on trips?

No

Are users aware of the acceptable, authorised use of a 'works' mobile?

The school does not have a works mobile.

How is this use monitored and recorded?

N/A

How do you ensure that the device is always ready for use e.g. fully charged and 'in credit'?

N/A

How are visitors, including parents made aware of your rules for acceptable use of a mobile phone?

Signs are positioned in the office area and staff will act if this is being flouted.

Are staff aware of the potential for mobile phones to be used for cyberbullying? How is cyberbullying approached in your school?

As part of our Curriculum / PSHE

Are staff aware that they may confiscate a phone or device if they believe it is being used to contravene the schools behaviour or bullying policy?

Yes

Do you have clear guidance regarding confiscating and searching the contents of a device or handing over evidence to police if you believe an illegal act has occurred?

Yes – it is within our school policy

Are staff vigilant in monitoring visitors for any covert use of mobile phones / cameras?

Yes

Do you have a procedure in place for reporting any suspicious use of mobile phones and / or cameras?

Are staff familiar with this? Yes, report to HT who will act on information and deal with as necessary.

Are users aware of any 'sanctions' for misuse of mobile phones?

Yes – it would result in disciplinary for a member of staff, and pupils are aware that misuse of mobile phones would result in the behaviour ladder consequences.

OTHER MOBILE DEVICES

As new technologies are introduced, their use should be risk assessed and balanced against their potential benefits for learning. If needed, amendments should be made to the e-Safety Policy.

In our school staff are allowed to make use of personal mobile devices in school in the following circumstances:

These devices must have security settings enabled e.g. access passwords

The device owners are aware of their responsibility to ensure all content on these devices is legal and appropriate for a school setting?

The device owners are aware that the school cannot be held liable e.g. for any damage or theft of personal devices?

If personal devices are to be connected to the Internet via the school's connection, they must be 'virus checked' (if applicable) before use on school systems

All school devices are stored in locked units and are all password protected. Content may be transferred between devices using encrypted storage or though "cloud storage," -this must be password protected and should never hold any personal information.

Inappropriate use of mobile devices would result in disciplinary procedures in line with our disciplinary policy.

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

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

We obtain written consent from parents for photographs of their children to be taken or used. Verbal consent is not considered acceptable.

Do you have written consent from adults employed in the setting for their photographs to be taken or used?

Yes - this is recorded on the A.U.P

It is made very clear, when gaining consent, how photographs can / cannot be used (including the use of external photographers or involvement of 3rd parties) Consent include permission to store / use images once a child has left the school e.g. for brochures, displays etc Parents should be informed of the timescale for which images will be retained. Permission is obtained yearly. Procedures are in place for changes in circumstances that may necessitate removal of permission. Permission lists are kept in class registers. Parents are informed of the purposes for which images may be taken and used e.g. displays, website, brochures, learning journeys and portfolios, press / other external media? Specific parental permission is required before child's images are included in portfolios maintained by trainees / students not directly employed by the setting.

Do you need permission to use group images in individual children's profiles e.g. can an image of a group activity in EYFS be included in several children's profiles?

Yes, has been incorporated in annual permission consent form.

How do you ensure that only current images are used, i.e. not children / adults who have left the setting?

Year 6 staff delete photos from server when class left. Monitoring of website by DHT & HT to ensure only photos of current images are being used.

The press have special permissions in terms of Data Protection and may wish to name individual children to accompany a photograph. Written permission from parents is required for this. At times, the media may publish an image in their online publication which may offer facilities for the 'public' to add comments in relation to a story or image. These can potentially invite negative as well as positive comments. Do you have parental permission for images to be used in a way that supports this?

Adults working in the setting are kept informed of any children / other adults whose photographs must not be taken through written and verbal means – Photo Permissions available in all registers.

Taking Photographs /Video

Which adults are authorised to take images?

No member of school staff will be authorised to take images if they have not been trained in E-safety. Any students etc are not allowed to take pictures – staff will take if necessary.

Are photographs/videos only taken using school owned equipment?

The use of personal equipment to store images should be avoided and deleted once on school server.

When taking photographs/ video, the rights of an individual to refuse to be photographed are respected?

We ensure that the photograph doesn't show children who are distressed, injured or in context that could be embarrassing or misinterpreted.   We ensure that certain children are not continually favoured when taking images

We ensure that subjects are appropriately dressed and not participating in activities that could be misinterpreted. This would include for example, considering the angle of shots for children engaged in PE activities.

Certain areas of the setting are 'off limits' for taking photographs, e.g. toilets, cubicles etc.

Close up shots should be avoided as these may be considered intrusive.

Shots should 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 of their own children on the provision that the images are for their own use, e.g. at a school production.

Note: Including other children or other purpose could constitute a potential breach of Data Protection legislation.

Parents are informed that they should only take photographs of their own children and that they need permission to include any other children.

Parents are reminded, on the annual consent form 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 school.

Do you have / need a request form that ‘allows’ parents to use cameras at a specified time / in a designated area for a particular purpose?

Yes – but we only use it if there is nothing else preventing cameras being used eg no permissions from some parents.

Parents encouraged to be considerate when taking photographs, e.g. not obscuring the view of others or being intrusive?

Yes

Storage of Photographs /Video

How do you ensure that photographs are securely stored and not removed from the school environment?

This could include storage of images on portable devices e.g. laptops or tablets. If unavoidable then images should be on password protected devices & stored securely. Once transferred to secure server images should be deleted.

Do you allow images to be stored on USB memory sticks? Are such mobile devices encrypted or password protected?

No, we do not allow images to be stored in USB or Memory sticks.

Do you ‘store’ images on tablets, ‘apps’ or use ‘Cloud’ storage? Are you confident that your images are being stored securely if hosted outside the setting?

No images on cloud storage. Pictures deleted from devices once they are on the server.

Are parents / carers informed if images are to be stored outside the school setting?

N/A

Do you allow staff to store images on personal equipment e.g. tablets, laptops or USB storage devices?

No

Do you allow staff to store personal images on school equipment?

No.

Who has access to photographs / videos stored on your equipment?

Only School staff who have access to the “teacher” drive.

Who is responsible for deleting photographs / video or disposing of printed copies (e.g. by shredding) once the purpose for the image has lapsed?

Each member of staff is responsible for own images.

How do you ensure images are disposed of should a parent withdraw permission?

Regular monitoring by HT/Bursar who have access to "photo permission" lists.

If you 'send' photographs electronically e.g. via email, how do you ensure that the e- mail is secure?

Staff must use "secure email" where possible or school email address (lancs.sch.uk).

Publication of Photographs /Videos

Consent is needed from parents for publication of children's images, e.g. on a website. Photographs should only be published online to secure sites. When publishing photographs, care should be taken over the choice of images to ensure that individual children / adults cannot be identified or their image made available for downloading or misuse, e.g. through the use of low definition images that will not magnify effectively.

- Full names and / or other personal information should not accompany published images.
- When publishing images, children's images must not be displayed on insecure sites e.g. personal Social Networking Sites
- Staff and children are aware that full names and personal details will not be used on any digital media, particularly in association with photographs
- All staff recognise and understand the risks associated with publishing images, particularly in relation to use of personal Social Network sites.
- Staff should ensure that personal profiles are secured and do not display content that is detrimental to their own professional status or could bring the school into disrepute.
- The Media, 3rd Parties and Copyright - Third Parties are supervised at all times whilst in the school and must comply with the Data Protection requirements in terms of taking, storage and transfer of images. Care must be taken with 3rd party as they will own the image. Only allow responsible 3rd parties who comply with Data Protection.
- If uploading images to a 3rd party website, e.g. for printing or creating calendars, cards etc, staff must read the terms and conditions of the web site. You could unknowingly be granting the site's host licence to modify copy or redistribute your images without further consent. The site may also be advertised for 'personal use' only – therefore using for business purposes would be a breach of the terms and conditions.

CCTV, Video Conferencing, VOIP and Webcams

- Parents should be informed if CCTV, video conferencing or webcams are being used in use in the school.
- Parental permission is required for any child/children to participate in activities that include taking of video and photographs. Although children may not be appearing 'live' on the Internet through a video conferencing link, it is still important to remember that the images which are broadcast from school could be captured as a snapshot or video clip from a system receiving the broadcast. Video conferencing (or similar) sessions are logged including the date, time and the name of the external organisation/ person(s) taking part?
- Notifications are in place to inform setting users that CCTV is being used.

- The purpose for using CCTV /video conferencing or webcams is made clear to those liable to be included in footage taken by these resources.
- Cameras are located in the corridors and the hall. They do not overlook sensitive areas, e.g. changing rooms or toilets. Recordings are stored on the camera system – which is password protected.
- Copyright, privacy and Intellectual Property Rights (IPR) legislation must be respected?
- Recordings must not be repurposed in any other form or media other than the purpose originally agreed - Image Consent forms can be found in the Appendices.

7. Communication technologies

We use a variety of communication technologies and all staff need to be aware of the benefits and associated risks. New technologies should be risk assessed against the potential benefits to learning and teaching before being employed throughout the school. Ideally this should be done before multiple devices are purchased. As new technologies are introduced, the e-Safety Policy should be updated and all users made aware of the changes. The following are examples of commonly used technologies included in our policy:

e-Safety Reviewed Date and where held

Email - all users have access to the Lancashire Grid for learning service as the preferred school email system. Staff should not use personal e-mail accounts during school hours

Do you have email accounts for children?

Children only have access to class email.

How are these organised e.g. class, group or project accounts?

Class email only Children at our school cannot be potentially identified through their email address e.g. john.smith@class6.myschool.co.uk

Only official email addresses should be used to contact staff or children. The virtue filtering service should reduce the amount of SPAM (Junk Mail) received on school email accounts.

Are all users aware of the risks of accessing content including SPAM, phishing, unsuitable materials and viruses from external email accounts, e.g. Hotmail or Gmail, in school? Yes Are all users aware that email is covered by The Data Protection Act (1988) and the Freedom of Information Act (2000), meaning that safe practice should be followed in respect of record keeping and security?

Yes

Are all users aware that all email communications may be monitored at any time in accordance with the Acceptable Use Policy?

Yes

How will the content of children's email communications be monitored?

Class email is monitored by class teacher.

How should users report any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature?

Report to a responsible adult as per A.U.P.

Are users aware that they should not open attachments that they suspect may contain illegal content as they could inadvertently be committing a criminal act?

Yes

Our school has elected to include a standard disclaimer at the bottom of all outgoing email communications (see below).

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 Holy Family Catholic 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 does not have a social network.
- The content on Social Network sites may be unmediated and inappropriate for certain audiences.
- If a Social Network site is used personally, details must not be shared with children and privacy settings be reviewed regularly to ensure information is not shared automatically with a wider audience than intended.
- They must not give personal contact details to pupils or parents/carers including mobile telephone numbers, details of any blogs or personal websites.
- The content posted online should not bring the school into disrepute or lead to valid parental complaints or be deemed as derogatory towards the school and/or its employees or be deemed as derogatory towards pupils and/or parents and carers or bring into question their appropriateness to work with children and young people.
- Adults must not communicate with children using any digital technology where the content of the communication maybe considered inappropriate or misinterpreted.
- Online Communications with parents, past pupils or siblings of pupils, especially if under the age of 18 should be discouraged.
- Children must not be added as 'friends' on any Social Network site.
- School would consider contacting the police in some events. Common concerns that may need consideration include:
- Posting inappropriate comments about staff or children that could be construed as instances of cyberbullying.
- Posting images of children or adults on profiles without permission of the individuals involved, especially if the photographs contain children other than their own.
- Instant Messaging or VOIP Instant Messaging systems, e.g. Text messaging, Skype, Facetime, are popular communication tools with both adults and children. They can provide an opportunity to communicate in 'real time' using text, sound and video. The filtering service 'blocks' some of these sites by default, but access permissions can be changed at the request of the headteacher.

- Are staff and children aware of the risks involved using this technology e.g. viewing inappropriate images or making unsuitable contacts – Yes through A.U.P. & regular communication with parents

Do you allow staff to use school equipment to communicate with personal contacts e.g. through 'Facetime' on an iPad?

No

Do you make use of more secure messaging, forum or chat systems within their VLE (e.g. Moodle)?

N/A

If the school uses text messaging to contact parents, how is the security of messages and data e.g. contact lists ensured?

- The school's texting system is only accessible to key staff who have individual log-ins & passwords.
- Virtual Learning Environment (VLE) / Learning Platform Various systems, e.g. Moodle are being used regularly in schools as communication tools. Your school should consider:
- How you manage the use of communication tools within the VLE.
- Who is given access and at what level?
- How passwords are issued and their security maintained.
- Which tools children are allowed to access.
- How children are taught to use these communication tools in a responsible way in conjunction with the e-Safety curriculum.

Whether teachers know how to monitor the use of these tools. if accounts are deleted when staff and children leave the school. Is this monitored and by whom?

N/A

Websites and other online publications - this may include for example, school websites, Social Network profiles, podcasts, videos, wikis and blogs. Information posted online is readily available for anyone to see and thus form an opinion about the school. From September 2012, the School Information (England) (Amendment) Regulations 2012 specified that certain up to date information must be made available on a school's website.

Only SBM, Admin staff & HT have access to edit online publications and ensure that the content is relevant and current. Our HT has overall responsibility for what appears on the website. No content is subject to copyright/personal intellectual property restrictions. None of the content is hidden behind a password protected area. Downloadable materials in a read-only format (e.g. PDF) where necessary, to prevent content being manipulated and potentially re distributed without the school's consent

8. Infrastructure and technology

We ensure that the infrastructure/network is as safe and secure as possible. Internet content filtering is provided by default. It is important to note that the filtering service offers a high level of protection but occasionally unsuitable content may get past the filter service. Sophos Anti-Virus software is included in the school's subscription, but this needs to be installed on computers in school and then configured to receive regular updates.

Children's access

All children supervised when accessing school equipment and online materials

Children have access to the school systems through class logins. Children's access is restricted to certain areas of the network.

Adult access

Adult access to school systems available for all staff is restricted according to their areas of responsibility.

Passwords

All users of the school network have a secure username and password

The administrator password for the school network is restricted to the administrators. Staff and children reminded of the importance of keeping passwords secure.   Passwords are changed regularly.

Software/Hardware

We have legal ownership of all software (including apps on tablet devices). The record of appropriate licenses for all software is maintained by the administrator. The administrator controls what software is installed on school systems.

Managing the network and technical support

Servers, wireless systems and cabling are securely located and physical access restricted. All wireless devices have security enabled.   Wireless devices are accessible only through a secure password.

Relevant access has been restricted on tablet devices e.g. downloading of apps or 'in- app' purchases.

The administrator is responsible for managing the security of your school network.

The safety and security of your school network is reviewed regularly School systems kept up to date in terms of security e.g. computers regularly updated with critical software updates/patches.

Users (staff, children, guests) have clearly defined access rights to your school network e.g. they have a username and password and with certain permissions assigned.

Staff and children required/reminded to lock or log out of a school system when a computer/digital device is left unattended.

Users are not allowed to download executable files or install software. The administrator is responsible for assessing and installing new software.

Users report any suspicion or evidence of a breach of security to the HT or DHT.

Using removable storage devices on school is only allowed if encrypted pen drives.

School equipment e.g. teachers laptop must not be used for personal/family use.

If network monitoring takes place, is it in accordance with the Data Protection Act (1998)?

Yes

Are staff made aware of all network monitoring and/or remote access that takes place and by whom?

Yes

All internal/external technical support providers are aware of your schools requirements / standards regarding e-Safety.

The headteacher, deputy headteacher and Bursar are responsible for liaising with/managing the technical support staff. Filtering is managed by the provider.

Staff are unable to access procedures for blocking and unblocking specific websites. Any requests should be made via the Headteacher/Deputy Headteacher or Bursar.

What procedures are there in place to ensure that ALL equipment including school laptops used at home are regularly updated with the most recent version of virus protection software used in school. All staff are requested to ensure their laptops are checked by the ICT administrator to ensure that the latest version of "Sophos" is installed & staff should ensure it is updating.

Staff should report any suspected or actual computer virus infection to the Headteacher/ Deputy Head Teacher and the Bursar.

9. Dealing with incidents

Our school has considered the types of incident that may occur and how these will be dealt with. An incident log (see Appendix 11) should be completed to record and monitor offences. This must be audited on a regular basis by a designated member of the Senior Leadership Team.

Illegal offences

Any suspected illegal material or activity must be brought to the immediate attention of the headteacher who must refer this to external authorities, e.g. Police, CEOP, Internet Watch Foundation (IWF). Never personally investigate, interfere with or share evidence as you may inadvertently be committing an illegal offence. It is essential that correct procedures are followed when preserving evidence to protect those investigating the incident (See Appendix 12). Always report potential illegal content to the Internet Watch Foundation (http://www.iwf.org.uk) .They are licensed to investigate – schools are not!

Examples of illegal offences are:

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

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

Inappropriate use

It is likely that our school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with quickly and actions are proportionate to the offence. Staff to note procedures to be followed:

Incident Procedure

Procedure and Sanctions Accidental access to inappropriate materials Minimise the webpage/turn the monitor off/click the 'Hector Protector' button.

- Tell a trusted adult.
- Enter the details in the Incident Log and report to our filtering services if necessary
- Persistent 'accidental' offenders may need further disciplinary action.
- Using other people's logins and passwords maliciously.
- Deliberate searching for inappropriate materials.
- Bringing inappropriate electronic files from home.
- Using chats and forums in an inappropriate way.
- Inform SLT or designated e-Safety Champion.
- Enter the details in the Incident Log

Additional awareness raising of e-Safety issues and the AUP with individual child/class

More serious or persistent offences may result in further disciplinary action in line with Behaviour Policy.

Consider parent/carer involvement

Who is responsible for dealing with e-Safety incidents?

The member of staff supervising the child, IT subject leader and DSL.

All staff should be aware of the different types of e-Safety incident and how to respond appropriately e.g. illegal or inappropriate. We use the 'e-Safety Incident/ Escalation Procedures' document (See Appendix 12) as a framework for responding to incidents.

The school's Behaviour Policy should outline policy and procedures relating to the powers of 'search' referred to in the Education Act (2011). Items 'banned' in school may include for example, electronic devices such as mobile phone

10. Acceptable Use Policy (AUP)

An Acceptable Use Policy 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 used for Staff, Children and Visitors/Guests and must be signed and adhered to by users before access to technology is allowed.

This agreement is a partnership between parents/carers, children and the school to ensure that users are kept safe when using technology.

A list of children who, for whatever reason, are not allowed to access technology must be kept in school and made available to all staff.

A set of exemplar AUPs are provided in the appendices and you may find it helpful to refer to these and the additional points below when writing your school's AUP.

Our School AUPS :

- Reflect the content of the school's wider e-Safety Policy.

- Be regularly reviewed and updated
- Be regularly communicated to all users, particularly when changes are made to the e-Safety Policy/AUP.
- Be understood by each individual user and relevant to their setting and role/ responsibilities.
- Outline/summarise acceptable and unacceptable behaviour when using technologies as defined in the wider e-Safety Policy.
- Outline the ways in which users are protected when using technologies e.g. passwords, virus protection and filtering.
- Provide advice for users on how to report any failings in technical safeguards.
- Clearly define how monitoring of network activity and online communications will take place and how this will be enforced.
- Outline sanctions for unacceptable use and make all users aware of the sanctions (linked to our Behaviour Policy).
- Stress the importance of e-Safety education and its practical implementation.
- Highlight the importance of parents/carers reading and discussing the content of the AUP with their child.

11. Education and training

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

Area of Risk Example of Risk Content: Children need to be taught that not all content is appropriate or from 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 sites.

- 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
- Identity 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).
- e-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' e-Safety. Our school provides relevant, flexible and engaging e-Safety education to all children as part of their curriculum entitlement

At Holy Family Catholic Primary School we provide regular, planned e-Safety teaching within a range of curriculum areas (using the Lancashire ICT Progression document) mainly taught in class, PSHE & assemblies

How do you ensure e-Safety education is progressive throughout the school?

We use eSafety advice and lesson plans from https://www.childnet.com/resources/the-adventures-of-kara-winston-and-the-smart-crew/smart-crew-guidance-and-activities

How will e-Safety education be differentiated for children with special educational needs?

Through adult support.

Do you have an additional focus on e-Safety during the National e-Safety Awareness Week?

We have an annual focus on E safety , but this is not necessarily during e safety week

How do you ensure children are made aware of the relevant legislation when using the Internet e.g. Data Protection Act (1998) and copyright implications?

Through monitoring children in class when using the internet.

Are children made aware of the impact of cyberbullying and how to seek help if they are affected by these issues, e.g. using peer mentoring or worry boxes?

Yes Worry boxes in each class. Anti bullying each year includes cyber bullying.

Are children taught to critically evaluate materials and develop good research skills through cross curricular teaching and discussions?

At an appropriate level - YES

Do you ensure that children develop an understanding of the importance of the Acceptable Use Policy and are encouraged to adopt safe and responsible use of ICT both within and outside school?

Yes through AUP and class discussion about safety, children are reminded of safe Internet use e.g. classroom displays, e-Safety rules (See Appendices).

e-Safety – Raising staff awareness

Staff training has been carried out to ascertain the level of knowledge and expertise in the use of new technologies and their potential benefits and risks.

Following a visit form an external e-Safety accredited provider & attendance on an e-Safety course HT & SBM prepared & delivered e-Safety training to staff & governors in September 2015.

Do any of your staff have accredited e-Safety qualifications e.g. EPICT or CEOP Ambassador?

No

During our e-Safety training we ensure staff are made aware of issues which may affect their own personal safeguarding e.g. use of Social Network sites.

All staff are expected to promote and model responsible use of ICT and digital resources.

E-Safety training is provided within an induction programme for all new staff to ensure that they fully understand both the school's e-Safety Policy and Acceptable Use Policy

Regular updates on e-Safety Policy, Acceptable Use Policy, curriculum resources and general eSafety issues are discussed in staff/team meetings.

E-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).

We offer regular opportunities for parents/carers and the wider community to be informed about eSafety, including the benefits and risks of using various technologies both at home and at school - through school newsletters, Website, Bespoke Parents e-Safety Awareness session workshops and promotion of external e-Safety resources/online materials.

E-Safety – Raising Governors' awareness

Governors, particularly those with specific responsibilities for e-Safety, ICT or child protection, are kept up to date. This may be through discussion at Governor meetings, attendance at Local Authority Training, CEOP or internal staff/parent meetings.

Ten governors also attended a session specifically for them & staff in June 2015 organised through our County provider.

NB: The e-Safety Policy should be regularly reviewed and approved by the governing body.

12. Evaluating the impact of the e-Safety Policy

It is important that schools monitor and evaluate the impact of safeguarding procedures throughout schools. Our evaluation will consider:

- How are e-Safety incidents monitored, recorded and reviewed? On concern sheets
- Who is responsible for monitoring, recording and reviewing incidents? HT / DHT/ Bursar
- Is the introduction of new technologies risk assessed? Yes
- Are these assessments included in the e-Safety Policy? NO – not currently , but will be in future
- Are incidents analysed to see if there is a recurring pattern e.g. specific days, times, classes, groups and individual children? Will be!

QUESTIONS TO CONSIDER

How can these patterns be addressed most effectively e.g. working with a specific group, class assemblies, reminders for parents? - through 1;1 , groups, class, whole school, training sessions

How does the monitoring and reporting of e-Safety incidents contribute to changes in policy and practice? - Any incidents would lead to a review and then possibly a change in policy/procedure

How are staff, parents/carers, children and governors informed of changes to policy and practice?

Through e- mail, APP, website , newsletter , face to face

How often are the AUPs reviewed and do they include reference to current trends and new technologies? Annually See Appendix 13.

APPENDIX 1 Image Consent Letter to Parents

Dear Parent / Carer

We regularly take photographs/videos of children at our school and believe that these can provide a valuable record of children's learning. These may be used in children's learning journeys and profiles, our school prospectus, in other printed publications, on our school website/VLE, or in school displays, including digital photo frames. (List any other specific uses here). We also actively encourage children to use school cameras to take photographs / videos as part of their learning activity. Occasionally, our school may be visited by the media or third party who will take photographs/videos of an event or to celebrate a particular achievement. These may then appear in local or national newspapers, websites or on televised news programmes.

We recognise that increased use of technology and opportunities for online publishing mean that there is greater potential for accidental or deliberate misuse. We endeavour to minimise risks by putting safeguards in place that will protect your child's interests, and enable us to comply with the Data Protection Act (1998). Please read and complete the attached consent form (for each child) and return to school as soon as possible. We appreciate that some families may have additional concerns and anxieties regarding protection of a child's identity and therefore request that you inform us, in writing, of any special circumstances either now or at any time in the future that may affect your position regarding consent.

APPENDIX 2   Image Consent Form

Name of the child's Parent/carer …………………………………………………………

Name of child ……………………………………………………………………………….

Year group ....

Please read the Conditions of Use on the back of this form then answer questions 1-4 below. The completed form (one for each child) should be returned to school as soon as possible. (Please Circle your response)

1. Do you agree to photographs / videos of your child being taken by authorised staff within the school?

Yes	No

2. Do you agree to photographs / videos of your child being taken in group situations by 3rd parties at special events e.g. School productions or extra-curricular events?

Yes	No

3. May we use your child's image in printed school publications and for digital display purposes within school?

Yes	No

4. May we use your child's image on our school's online publications e.g. website / blog / VLE?

Yes	No

5. May we record your child on video?

Yes	No

6. May we allow your child to appear in the media as part of school's involvement in an event?

Yes	No

I have read and understand the conditions of use attached to this form

Parent/Carer's signature: ………………………………………………………………..

Name (PRINT):……………………………………………………… Date ………………..

1. This form is valid for this academic year.

2.The school will not re-use any photographs or videos after your child leaves this school without further consent being sought.

3. The school will not use the personal contact details or full names (which means first name and surname) of any pupil or adult in a photographic image, or video, on our website/VLE or in any of our printed publications.

4. If we use photographs of individual children, we will not use the full name of that pupil in any accompanying text or caption.

5. If we use the full name of a pupil in the text, we will not use a photograph of that pupil to accompany the article.

6. We will only use images of children who are suitably dressed and in a context that is not open to misinterpretation.

7. Third Parties may include other children's parents or relatives e.g. attending a school production.

8. Images / videos will be stored according to Data Protection legislation and only used by authorised personnel.

9. Parents should note that websites can be viewed throughout the world and not just in the United Kingdom, where UK law applies.

Notes on Use of Images by the Media If you give permission for your child's image to be used by the media then you should be aware that: 1. The media will want to use any images/video that they take alongside the relevant story. 2. It is likely that they will wish to publish the child's full name, age and the school's name in the caption for the picture (possible exceptions to this are large group or team photographs). 3. It is possible that the newspaper will re-publish the story on their website or distribute it more widely to other newspapers or media organisations.

APPENDIX 3

Consent Form for Images to be taken e.g. at a School Production or Special Event

Dear Parent/ Carer,

Your child will be appearing in our school production/event name on.

We are aware that these events are special for children and their relatives/friends and form treasured memories of their time at school.

We have a rigorous policy in place with regard to taking, using and publishing images of children and you have already signed a consent form stating whether you agree to your child's images/video being used in general circumstances.

Many parents/carers like to take photographs/videos of their children appearing in school productions, but there is a strong possibility that other children may be included in the pictures. In these circumstances, we request specific consent for images/videos to be taken by a third party (i.e. other parents). We need to have permission from all parents/carers of children involved in the production to ensure that they are happy for group images/videos to be taken and I would be grateful if you could complete the slip at the bottom of this letter and return to school as soon as possible.

We would also request that images/videos including other children or adults are not posted online, especially on Social Media sites e.g. Facebook, without the specific permission of the individuals included in the footage. Should any parents/carers not consent, we will consider other options, e.g. arranging specific photo opportunities after the production. These decisions are not taken lightly, but we have to consider the safeguarding of all our children and respect parents' rights to privacy.

Child's name: ______________________________ Date: ____________________

I agree/do not agree to photographs/videos being taken by third parties at the

………………………………………… on ………..…………………………………………..

Signed____________________________________ (Parent/Carer

Print name _______________________________

APPENDIX 4 Example of ICT Acceptable Use Policy (AUP) – Staff and Governors

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

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

- I will take responsibility for my own use of any technologies, making sure that I use them safely, responsibly and legally.
- I will be an active participant in e-Safety education, taking personal responsibility for my awareness of the opportunities and risks posed by the use of technology.
- I will not use communications devices, whether school provided or personally owned, for bullying or harassment of others in any form.
- I will not be involved with any online activities, either within or outside school that may bring the school, staff, children or wider members into disrepute. This includes derogatory/inflammatory comments made on Social Network Sites, Forums and Chat rooms.
- I will not browse, download/upload or distribute any material that could be considered offensive, illegal or discriminatory.
- I will respect copyright and intellectual property rights. 7. I will ensure that all electronic communications with children and other adults are appropriate.
- I will not use the school system(s) for personal use during working hours.
- I will not install any hardware or software without the prior permission of the Headteacher .
- I will ensure that personal data (including data held on MIS systems) is kept secure at all times and is used appropriately in accordance with Data Protection legislation.
- I will ensure that images of children and/or adults will be taken, stored and used for professional purposes in line with school policy and with written consent of the parent/carer or relevant adult. I will not distribute images outside the school network without the prior permission of the parent/carer, or person/s in the image.
- I will abide by the school’s rules for using personal mobile equipment, including my mobile phone, at all times.
- I will report any known misuses of technology, including the unacceptable behaviours of others.
- I have a duty to respect the technical safeguards which are in place. I understand that attempting to breach technical safeguards or gain unauthorised access to systems and services is unacceptable.
- I have a duty to report failings in technical safeguards which may become apparent when using the systems and services.
- I have a duty to protect passwords and personal network logins, and should log off the network when leaving workstations unattended. I understand that any attempts to access, corrupt or destroy other users’ data, or compromise the privacy of others in any way, using any technology, is unacceptable.

- I understand that network activities and online communications are monitored, including any personal and private communications made using school systems.
- I am aware that in certain circumstances where unacceptable use is suspected, enhanced monitoring and procedures may come into action, including the power to confiscate personal technologies such as mobile phones.
- I will take responsibility for reading and upholding the standards laid out in the AUP. I will support and promote the school's e-Safety policy and help children to be safe and responsible in their use of ICT and related technologies.
- I understand that these rules are designed for the safety of all users and that if they are not followed, school sanctions will be applied and disciplinary action taken.
- I give my consent to my photograph being on display around school & on the school's website.

User Signature

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

Signature ……..

Date …….

Full Name ……

(PRINT) Position/Role …….

APPENDIX 5

Students, Supply Teachers, Visitors & Guests etc.

To be signed by any adult working in the school for a short period of time.

- I will take responsibility for my own use of any technologies, making sure that I use them safely, responsibly and legally.
- I will not browse, download/upload or distribute any material that could be considered offensive, illegal or discriminatory.
- I will not use any external device to access the school's network e.g. pen drive.
- I will respect copyright and intellectual property rights.
- I will ensure that images of children and/or adults will be taken, stored and used for professional purposes in line with school policy and with written consent of the parent/carer or relevant adult. I will not distribute images outside the school network without the prior permission of the parent/carer, or person/s in the image.
- I will abide by the school's rules for using personal mobile equipment, including my mobile phone, at all times.
- I understand that network activities and online communications are monitored, including any personal and private communications made using school systems.
- I will not install any hardware or software onto any school system
- I understand that these rules are designed for the safety of all users and that if they are not followed, school sanctions will be applied and disciplinary action taken.

User Signature

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

Signature ……..

Date ………..

Full Name ………(PRINT)

Position/Role …….

Appendix 6 ICT Acceptable Use Policy (AUP) - Children

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

- I will only use ICT in school for school purposes. I will not bring equipment e.g. a mobile phone or mobile games consoles into school unless specifically asked by my teacher.
- I will only use the Internet and/or online tools when a trusted adult is present.
- I will only use my class e-mail address or my own school email address when emailing.
- I will not deliberately look for, save or send anything that could be unpleasant or nasty.
- I will not deliberately bring in inappropriate electronic materials from home.
- I will not deliberately look for, or access inappropriate websites.
- If I accidentally find anything inappropriate I will tell my teacher immediately.
- I will only communicate online with people a trusted adult has approved.
- I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.
- I will not give out my own, or others’, details such as names, phone numbers or home addresses.
- I will not tell other people my ICT passwords. I will not arrange to meet anyone that I have met online.
- I will only open/delete my own files.
- I will not attempt to download or install anything on to the school network without permission.
- I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
- I know that my use of ICT can be checked and that my parent/ carer contacted if a member of school staff is concerned about my e-Safety.
- I understand that failure to comply with this Acceptable Use Policy may result in disciplinary steps being taken in line with the school’s Behaviour Policy.

……………………………………………………………………………………Parent/ Carer signature

We have discussed this Acceptable Use Policy and

……………………………….................................... [Print child’s name]

agrees to follow the e-Safety rules and to support the safe use of ICT at all times.

Parent /Carer Name (Print) ……………………………………………………………………………….…………….

Parent /Carer (Signature) ……………………………………………………………..………….

Class ……………………………………………. Date……………………….……………………………………

This AUP must be signed and returned before any access to school systems is allowed.

APPENDIX 7 ICT Acceptable Use Policy (AUP) Parent's Letter

Dear Parent/Carer,

The use of ICT including the Internet, e-mail, learning platforms and mobile technologies are integral elements of learning in our school.

To make this as successful and as beneficial as possible for all learners, we expect all children to act safely and responsibly when using technology both within, and outside of, the school environment.

In school, we ensure that all resources used by the children are age appropriate and suggest that parents check the terms and conditions for the use of online resources and games to ensure that resources used at home are also age appropriate.

This is particularly relevant when using Social Network Sites that incorporate age-restriction policies where the minimum acceptable age is 13 years. Any child who sets up or uses such a site and is below the acceptable age is in clear breach of the site's privacy policy and / or terms and conditions and therefore we actively discourage this in our school.

The enclosed ICT Acceptable Use Policy forms part of the wider School e-Safety Policy and alongside the school's Behaviour and Safeguarding Policies outlines those principles we expect our children to uphold for the benefit of both themselves and the wider school community. Your support in achieving these aims is essential and I would therefore ask that you please read and discuss the enclosed ICT Acceptable Use Policy with your child and return the completed document as soon as possible.

Signing the School Acceptable Use Policy helps us to maintain responsible use of ICT and safeguard the children in school. Along with addressing e-Safety as part of your child's learning, we will also be holding Parental e-Safety Awareness Sessions during the school year and I would take this opportunity to strongly encourage your attendance wherever possible. Further information on these sessions will be communicated as soon as dates are confirmed.

In the meantime, if you would like to find out more about e-Safety for parents and carers, please visit the Lancsngfl e-Safety website http://www.lancsngfl.ac.uk/e-Safety If you have any concerns or would like to discuss any aspect of the use of ICT in school, please contact the headteacher.

Yours sincerely,

APPENDIX 8 Example of Typical Classroom e-Safety Rules (EYFS/KS1)

Our Golden Rules for Staying Safe with ICT

We only use the Internet when a trusted adult is with us.

We are always polite and friendly when using online tools.

We always make careful choices when we use the Internet.

We always ask a trusted adult if we need help using the Internet.

We always tell a trusted adult if we find something that upsets us.

APPENDIX 9   Example of Typical Classroom e-Safety Rules   (KS2)

Our Golden Rules for Staying Safe with ICT

We immediately close/minimise any page we are uncomfortable with (or if possible switch off the monitor).

We always ask permission before using the internet.

APPENDIX 10

Example of Letter to Parents Regarding Parental e-Safety Awareness Session

Dear Parent/Carer,

Having access to online information and the opportunities that the digital world can offer has many benefits and for some it plays an important part of our everyday lives. However, as technology moves on at such a pace, it is sometimes difficult to keep up with new trends and developments, particularly with regard to mobile/games technologies and secure and safe accessibility to online material.

Our school has policies in place to ensure our children are learning in a safe and secure environment which includes being safe online. This session has been organised to help you to contribute to the process of helping your child to be aware of the potential risks associated with using the Internet and modern technologies. Ofsted increasingly view Parental e-Safety Awareness sessions as essential components of effective safeguarding provision and I would therefore appreciate your support in attending this event.

We will be hosting the above session on the Date/Time below and I would strongly encourage your attendance: Date:…………………………………………………..Time:…………………………………………………………

The session will include reference to the following areas with time for you to ask questions: What are our children doing online and are they safe? Do they know what to do if they come across something suspicious? Are they accessing age-appropriate content? How can I help my child stay safe online? The session will last for approximately 1¼ hrs where a member of the Local Authority Schools' ICT Team will address the issues mentioned above.

Yours sincerely,

I / we will be attending the above Parental e-Safety Awareness Session

Name(s):……

Parent / Carer of:…………………………………………………………………Year

Incident Log

All e-Safety incidents must be recorded by the School e-Safety Champion or designated person. This incident log will be monitored and reviewed regularly by the Headteacher and Chair of Governors.

Date and Time of Incident

Type of Incident

Name of pupil/s and staff involved

System details

Incident detail Resulting actions taken and by whom (and signed)

Example only

Sept 2018 9.50 am

Accessing Inappropriate Website

A N Other (Pupil) A N Staff (Class Teacher)

Class 1 Computer

5 Pupil observed by Class Teacher deliberately attempting to access adult websites

Pupil referred to Headteacher and given warning in line with sanctions policy for 1st time infringement of AUP.

Site reported to Virtue inappropriate

APPENDIX 12 Responding to e-Safety Incident/ Escalation Procedures (see folder)

APPENDIX 13

EVALUATION of e-Safety PROCEDURES AND POLICY

How are e-Safety incidents monitored, recorded and reviewed?

Recorded on log sheet. Monitored by HT

Who is responsible for monitoring, recording and reviewing incidents?

e-Safety Campion, HT & Governors from the S & E committee

Is the introduction of new technologies risk assessed?

Yes

Are these assessments included in the eSafety Policy?

Not currently @ Sept 2018 but will be in future

Are incidents analysed to see if there is a recurring pattern e.g. specific days, times, classes, groups and individual children?

Will be when new log is in place

How can these patterns be addressed most effectively e.g. working with a specific group, class assemblies, reminders for parents?

Assemblies, e-Safety curriculum, website, groups

How does the monitoring and reporting of eSafety incidents contribute to changes in policy and practice?

Highlights vulnerable areas – leads to review

How are staff, parents/carers, children and governors informed of changes to policy and practice?

School App & website, weekly news, text message & meetings.

How often are the AUPs reviewed and do they include reference to current trends and new technologies?

A.U.Ps are reviewed annually & reference current trends & technologies