ONLINE SAFETY & ACCEPTABLE USE POLICY

September 2024

Reviewed by Governors	September 2024	Signed: 
Next Review date	September 2025	

Contents

<u>Appendices</u>

Introduction

New technologies inspire children to be creative, communicate and learn. However, while the internet is a great resource, it is important that children and young people are protected from the risks they may encounter. Holy Family Primary School endeavours to highlight benefits and risks of using technology and provides Safeguarding and education for users to enable them to control their online experience.

Computing and ICT covers a wide range of resources including; web-based and mobile learning. It is important to recognise the constant and fast paced evolution of technology within our society as a whole. Currently, the internet technologies children and young people are using both inside and outside of the classroom include (but are not limited to):

- Websites
- Learning platforms and virtual learning environments
- Email and instant messaging
- Chat rooms and social networking
- Blogs and wikis
- Podcasting
- Video broadcasting
- Music downloading
- Gaming and gaming devices
- Mobile/smart phones with text, video and/or web functionality
- Other mobile devices with web functionality

Whilst exciting and beneficial both in and out of the context of education, much of technology, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of online technologies. The breadth of issues classified within e-safety are considerable, but can be categorised into three areas of risk:

- Content: being exposed to illegal, inappropriate or harmful material
- Contact: being subjected to harmful online interaction with other users
- Conduct: personal online behaviour that increases the likelihood of, or causes harm.
- Commerce: risk from things like online gambling, inappropriate advertising, phishing or financial scams.

At Holy Family Primary School, we understand the responsibility to educate our pupils on these areas of risk; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Both this policy and the Acceptable Use Agreement (for all staff, governors, volunteers, visitors and pupils) are including of fixed and mobile internet technologies provided by the school (such as PC's, laptops, tablets, webcams, whiteboards, digital video equipment, etc).

Disclaimer: Due to the constant changes taking place within technology, this policy may not contain the most recent developments. We will, however, endeavour to add any important issues to the policy on our website.

Aims

Holy Family Primary School aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers, visitors and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

Legislation and Guidance (See Appendix 7)

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education KCSIE (2020) – (Annex C), and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Searching, screening and confiscation

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

Roles and Responsibilities

This policy, supported by the school's Acceptable Use Agreements for staff, governors, visitors and pupils, is to protect the interests and safely of the whole school community. It is linked to the following mandatory school policies: Child Protection, Health and Safety, Home School Child Agreement, Behaviour Policy (including the anti-bullying) and PSHE.

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation. The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL). All governors will ensure that they have read and understand this policy and agree and adhere to the terms on acceptable use of the school's ICT systems and the internet.

The headteacher (Grainne Griffiths) is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

The Deputy designated safeguarding lead (Clare Twycross) and e-safety coordinator (Sarah Thompson) take lead responsibility for online safety in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Keep abreast of current issues and guidance through organisations such as CEOP (Child Exploitation and Online Protection, NSPCC and Child.net.
- Working with the headteacher, Computing subject leader and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy

- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet and ensuring that pupils follow the school's terms on acceptable use
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

Parents are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use.

E-Safety Skills Development for Staff

Our staff receive regular information and training on e-safety issues in the form of staff meetings and notices. Details of staff training can be obtained from the school's e-safety coordinator. New staff receive information on the school's Acceptable Use policy (See Appendix 1) as part of their induction. All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of e-safety and know what to do in the event of misuse of technology by any member of the school community. All staff are to incorporate e-safety activities and build awareness by following the Computing scheme of work and supporting 'Safer Internet Day' yearly.

Educating Pupils about Online Safety

Holy Family Primary School provides opportunities within a range of curriculum areas to teach about e-safety including discrete e-safety objectives within the Computing curriculum. Educating pupils on the dangers of technologies that maybe encountered outside school is done informally when opportunities arise and as part of the curriculum.

Pupils will be taught about online safety as part of the curriculum. From September 2020 all schools will have to teach 'Relationships education and health education in primary schools (RSE).' This new requirement includes aspects about online safety.

In Early Years and Key Stage 1, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

In Key Stage 2, pupils will be taught to:

- Use technology safely, respectfully and responsibly

- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

By the end of primary school, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not.
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

The safe use of social media and the internet will also be covered in other subjects where relevant.
The school will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

Educating Parents about Online Safety

Holy Family Primary School will raise parents' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents. Online safety will also be covered during parents' evenings. If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL. Concerns or queries about this policy can be raised with any member of staff or the headteacher.

Cyber-Bullying

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school Behaviour policy.)

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.
The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will discuss cyber-bullying with their pupils and the issue will be addressed in assemblies.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained. The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so. When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police

Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation. Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

Managing the Internet

The internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people. All use of the internet is logged and the logs are randomly but regularly monitored. Whenever any inappropriate use if detected, it will be followed up.

The school maintains students will have supervised access to internet resources (where reasonable) through the schools fixed and mobile internet technology. Staff will previous any recommended sites before use. All users must observe software copyright at all times. It is illegal

Filtering

The school filtering and monitoring provision is agreed by senior leaders, governors and the IT Provider and is regularly reviewed (at least annually) and updated in response to changes in technology and patterns of online safety incidents/behaviours.

Day to day management of filtering and monitoring systems requires the specialist knowledge of both safeguarding and IT staff to be effective. The DSL will have lead responsibility for safeguarding and online safety and the IT service provider will have technical responsibility, the filtering and monitoring provision is reviewed (at least annually) by senior leaders, the Designated Safeguarding Lead and a governor with the involvement of the IT Service Provider.

- checks on the filtering and monitoring system are carried out by the IT Service Provider with the involvement of a senior leader, the Designated Safeguarding Lead and a governor, in particular when a safeguarding risk is identified, there is a change in working practice, e.g. remote access or new technology is introduced.
- the school manages access to content across its systems for all users and on all devices using the schools internet provision. The filtering provided meets the standards defined in the DfE Filtering standards for schools and colleges and the guidance provided in the UK Safer Internet Centre Appropriate filtering.
- illegal content (e.g., child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation URL list and the police assessed list of unlawful terrorist content, produced on behalf of the Home Office. Content lists are regularly updated
- there are established and effective routes for users to report inappropriate content, recognising that no system can be 100% effective
- there is a clear process in place to deal with, and log, requests/approvals for filtering changes (see Appendix for more details).
- filtering logs are regularly reviewed and alert the Designated Safeguarding Lead to breaches of the filtering policy, which are then acted upon.
- the school has a mobile phone policy and where personal mobile devices have internet access through the school network, content is managed in ways that are consistent with school policy and practice.
- access to content through non-browser services (e.g. apps and other mobile technologies) is managed in ways that are consistent with school policy and practice.

If necessary, the school will seek advice from, and report issues to, the SWGfL Report Harmful Content site.

Monitoring

The school has monitoring systems in place to protect the school, systems and users:

- The school monitors all network use across all its devices and services.
- monitoring reports are urgently picked up, acted on and outcomes are recorded by the Designated Safeguarding Lead, all users are aware that the network (and devices) are monitored.
- There are effective protocols in place to report abuse/misuse. There is a clear process for prioritising response to alerts that require rapid safeguarding intervention.
- Management of serious safeguarding alerts is consistent with safeguarding policy and practice.

The school follows the UK Safer Internet Centre Appropriate Monitoring guidance and protects users and school systems through the use of the appropriate blend of strategies informed by the school's risk assessment. These may include:

- physical monitoring (adult supervision in the classroom)
- internet use is logged, regularly monitored and reviewed
- filtering logs are regularly analysed and breaches are reported to senior leaders
- pro-active alerts inform the school of breaches to the filtering policy, allowing effective intervention.
- where possible, school technical staff regularly monitor and record the activity of users on the school technical systems

- use of a third-party assisted monitoring service to review monitoring logs and report issues to school monitoring lead(s)

Infrastructure

Coventry has a monitoring solution where web-based activity is monitored and recorded. School internet access is controlled through Smooth Wall, the LA's web filtering service. Our school has the facility for further customization of the web filtering. This is the responsibility of the e-Safety co-ordinators. Holy Family Catholic Primary is aware of its responsibility when monitoring staff communication under current legislation and takes into account; Data Protection Act 2018, The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Regulation of Investigatory Powers Act 2000, Human Rights Act 1998.

Staff and pupils are aware that school based email and internet activity can be monitored and explored further if required. The school does not allow pupils access to internet logs. If staff or pupils discover an unsuitable site, the screen must be switched off, or closed, and the incident reported immediately to the teacher and then to the e-safety co-ordinator. All e-Safety related incidents are logged down. It is the responsibility of the school, by delegation to the network manager Dale Vernon, (Hybrid Media) to ensure that Anti-virus protection is installed on all school machines. This automatically updates.

Pupils and Staff using personal removable media are responsible for measures to protect against viruses, for example making sure that additional systems used have up-to-date virus protection software. It is not the school's responsibility nor the network managers to install or maintain virus protection on personal systems.

Pupils and staff are not permitted to install programs or files on school based technologies.

If there are any issues related to viruses or anti-virus software, the e-Safety co-ordinator should be informed.

Mobile Technologies

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. Many existing mobile technologies such as tablets, notebooks (laptops), gaming devices, and Smartphones are familiar to children outside of school too. They often provide a collaborative, well-known device with possible internet access but also open up the risks, and potential misuse, of communication and internet technologies. Emerging technologies are continually examined for educational benefit and their potential risks evaluated. In order to ensure appropriate use of these devices, our school chooses to manage them in the following ways:

Personal Mobile Devices (including phones)

The school allows staff to bring in personal mobile phones and devices for their own use. Under certain circumstances the school allows a member of staff to contact a pupil or parent/ carer using their personal device. The school is not responsible for the loss, damage or theft of any personal mobile device. The sending of inappropriate text messages between any member of the school community is not allowed. Permission must be sought before any images, videos or sound recordings are made on these devices by any member of the school community. Users bringing personal devices into school must ensure that these are free of inappropriate or illegal content. Staff are asked to turn off mobiles during teaching times. If a

member of staff is expecting an important call he/she must inform the head teacher and phase leader so that the phone can be turned on and checked. Where the school provides mobile technologies such as phones, laptops and tablets for offsite visits and trips, only these devices should be used. Where the school provides a laptop for staff, only this device may be used to conduct school business outside of school.

Managing Email

The use of email within most schools is an essential means of communication for both staff and pupils. As part of the school's curriculum, email can offer significant benefits including; direct written contact between schools on different projects, be they staff based or pupil based, within school or international. We recognise that pupils need to understand how to style an email in relation to their age and use good 'netiquette'. In order to achieve higher standards of ICT and Computing, pupils must have experienced sending and receiving emails. Pupils are taught, either discretely or as part of other curriculum areas, how to send and receive emails within the Computing curriculum.

The school gives all staff their own email account to use for all school business. This is to minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed. It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary email histories can be traced. In the context of school, email should not be considered private. This should be the account that is used for all school business.

Under no circumstances should staff contact pupils, parents or conduct any school business using personal email addresses.

The school requires a standard disclaimer to be attached to all email correspondence, stating that, 'the views expressed are not necessarily those of the school or the Local Authority'. The responsibility for adding this disclaimer lies with the account holder.

E-mail sent to an external organisation should be written carefully before sending, in the same way as any letter written on school headed paper.

Pupils may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes.

All e-mail users are expected to adhere to the generally accepted rules of network etiquette. Particularly in relation to the use of in-appropriate language and the sharing of personal details, both of themselves and others.

All known attachments should be checked for viruses and unexpected or ambiguous attachments should not be opened.

Pupils must inform a teacher, or a trusted adult, if they receive an offensive e-mail. Staff must inform the e-Safety co-ordinator or their line-manager, if they receive an offensive e-mail.

Safe Use of Images (See Appendix 4)

<u>Taking of Images and Film</u>
Digital images are easy to capture, reproduce and publish. However, they are also easy to misuse. It may not always be appropriate to take or store images of any member of the school community or public.

Consent must always be sought before-hand and one must always consider the appropriateness of, and the audience for, these images.

With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment.

Staff are not permitted to use personal equipment, such as mobile phones and cameras, to record images of pupils. This also includes residential and field trips. However, with the express permission of the Head teacher, images can be taken provided they are transferred immediately and solely to the school's network and then deleted from the staff member's device.

Consent of adults who work at the school

Permission to use images of all staff who work at the school is sought on induction and a copy is kept in their personnel file

Publishing pupil's images and work

On a child's entry to the school, all parents/guardians will be asked to give permission to use their child's work/photos in the following ways:

- On the school web site
- On the school's Learning Platform
- In the school prospectus and other printed publications that the school may produce for promotional purposes
- Photographs and videos published via social media sites such as the school's official Twitter or YouTube accounts.
- In display material that may be used in the school's communal areas
- In display material that may be used in external areas, i.e. exhibition promoting the school
- General media appearances, e.g. local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically)

This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue, e.g. divorce of parents, custody issues, etc.

Parents/ carers may withdraw permission, in writing, at any time.

Storage of Images

Images/ films of children are stored on the Admin computers. Pupils and staff are not permitted to use personal portable media for storage of images (e.g., USB sticks) without the express permission of the Head teacher. Rights of access to this material are restricted to the teaching staff and pupils within the confines of the school network/ Learning Platform. School office staff only have the responsibility of deleting the images when they are no longer required, or when the pupil has left the school.

Webcams and CCTV

We do not use publicly accessible webcams in school. Webcams in school are only ever used for specific learning purposes, i.e. monitoring chicks hatching and never using images of children or adults. Misuse of the webcam by any member of the school community will result in sanctions.

Video Conferencing (Not applicable)

All pupils are supervised by a member of staff when video conferencing. All pupils are supervised by a member of staff when video conferencing with end-points beyond the school. Approval from the Head teacher is sought prior to all video conferences within school. No part of any video conference is recorded in any medium without the written consent of those taking part.

Additional points to consider:

- Participants in conferences offered by 3rd party organisations may not be checked for a valid DBS.
- Conference supervisors need to be familiar with how to use the video conferencing equipment, particularly how to end a call if at any point any person taking part becomes unhappy with the content of the conference.

Acceptable Use of the Internet in School

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet. Visitors will be expected to read and agree to the school's terms on acceptable use if relevant. Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role. We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

Pupils are provided with a Learning Platform log-in username. Pupils are taught to keep their usernames and passwords private. If pupils think their password may have been compromised or someone else has become aware of their password, they report this to their class teacher or e-safety coordinator.

Pupils are not allowed to deliberately access online materials or files on the school network, of their peers, teachers or others.

Staff are aware of their individual responsibilities to protect the security and confidentiality of school networks, MIS systems and/or Learning Platform, including ensuring that passwords are not shared and are changed periodically.

Staff using Work Devices outside School and Data Security

The accessing of school data is something that the school takes very seriously. The school follows 'Becta' guidelines (published Autumn 2008). Staff are aware of their responsibility when accessing school data. They must not:

- Access data out of school
- Take copies of data
- Allow others to view data
- Edit the data unless specifically requested to do so by the Head Teacher and/or Governing Body.

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use.

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. Any USB devices containing data relating to the school must be encrypted.

If staff have any concerns over the security of their device, they must seek advice from the e-safety coordinator.

Work devices must be used solely for work activities.

How the school will respond to issues of misuse (See Appendix 1, 2, 5)

Complaints relating to e-safety should be made to the teacher or Head Teacher. Incidents should be logged and the flowcharts for Managing an E-Safety Incident should be followed.

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on Behaviour and Internet Acceptable Use. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the Staff Code of Conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

Equal Opportunities – Pupils with Additional Needs

The school endeavours to create a consistent message with parents for all pupils and this in turn should aid establishment and future development of the school e-safety rules. However, staff are aware that some pupils may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of e-safety issues.

Where a pupil has poor social understanding, careful considering is given to group interactions when raising awareness of e-safety. Internet activities are planned and well managed for these children and young people.

Holy Family Primary School E-Safety Incident Log (See Appendix 5)

Details of all e-safety incidents to be recorded by all staff via Child Protection Online Monitoring Service (CPOMS). This incident log will be monitored by the Head Teacher and by governors via the Head Teachers Report to Governors.

Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation. All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

The DSL (Grainne Griffiths) will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our Child Protection and Safeguarding policy.

Parental Involvement

Parents/carers and pupils are actively encouraged to contribute to the school e-safety policy by letter and by reporting unsuitable sites etc to the e-safety coordinator. Parents/carers are asked to read through and sign the Acceptable Use Agreements of behalf of their child on admission to school. Parents/carers are required to make a decision as to whether they consent to images of their child being taken/used in the public domain (e.g. on the school website). The school disseminates information to parents relating to e-safety where appropriate in the form of:

- School website
- Newsletter items
- Parents/carers information meetings/evenings

Reviewing the Policy

Staff have been involved in making/reviewing the e-safety policy through staff meetings. There will be an on-going opportunity for staff to discuss with their phase leader/SLT any issues of e-safety that concerns them.

This policy will be reviewed every year by the e-safety coordinator and consideration will be given to the implications for future whole school development planning. The policy will be amended if new technologies are adopted or Central Government changes the orders or guidance in any way. At every review, the policy will be shared with the governing board.

Date approved by staff:

Date approved by governors:

Signed: **Review date:**

Appendix 1

Holy Family Primary School Acceptable Use Agreement/Code of Conduct: Staff, Governors and Visitors

ICT and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with S.Thompson/J.Richardson the school e-Safety coordinators.

Deliberate access to inappropriate materials by any user will lead to the incident being logged by the e-Safety co-ordinators, depending on the seriousness of the offence; investigation by the Head teacher/ LA, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences

- I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number and personal email address, to pupils.
- I will only use the approved, secure email system(s) for any school business.
- I will ensure that personal data (such as data held on SIMS) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Body.
- I will not install any hardware or software without seeking permission from the head teacher.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and/ or staff will only be taken, stored and used for professional purposes inline with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Head teacher.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Head teacher.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will support and promote the school's e-Safety policy and help pupils to be safe and responsible in their use of ICT and related technologies.

User Signature

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

Signature …… Date ……

Full Name …… (printed)

Job title ……

Appendix 2

Acceptable Use Agreement for All Pupils

I agree to follow the following e-Safety rules when using ICT

For my own personal safety:

- I understand that the school will monitor my use of computers.
- I will treat my username and password like my toothbrush – I will not share it, nor will I try to use any other person's username and password.
- I will be aware of "stranger danger", when using computers.
- I will not share personal information about myself or others when on-line.
- If I arrange to meet people off-line that I have spoken to on-line, I will do so in a public place and take an adult with me.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

I understand that everyone has equal rights to use technology as a resource and:

- I understand that the school computers are for educational/school use and that I will not use the computers unless I have permission to do so.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet space and stop others from being able to carry out their work.
- I will not use the school computers for on-line gaming, internet shopping, file sharing, or video broadcasting (e.g. YouTube), unless I have permission of a teacher to do so.

I know that the school has a responsibility to keep all pupils safe when using ICT:

- I will not use my personal hand held / external devices such as mobile phones / USB devices etc in school unless I have permission.
- I understand that, if I am allowed to use my own devices in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.
- I understand the risks and will not try to upload, download or access any materials which may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering / security systems in place.
- I will report any damage or faults involving equipment or software, however this may have happened.
- I will not open any attachments to emails, unless I know and trust the person who sent the email, due to the risk of the attachment containing viruses or other harmful programmes.
- I will not install or attempt to install programmes of any type on a machine, nor will I try to alter computer settings.

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

- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).
- I will only use chat and social networking sites with permission. (Parents should always check guidance on recommended ages, when allowing children supervised access to social networking sites.)

Dear Parent/ Carer,

ICT including the internet, email and mobile technologies etc. have become an important part of learning in our school. We expect all children to be safe and responsible when using any ICT.

If pupils fail to comply with this Acceptable Use Policy Agreement, they will be subject to the schools Behaviour Policy. (See attached) This may include loss of access to the school computers, time in or time out or may result in fixed term exclusion. Contact with parents and in the unlikely event of illegal activities involvement of the police will take place.

Please read and discuss these e-Safety rules with your child and return the slip at the bottom of this page. If you have any concerns or would like some explanation please contact the Head teacher

Pupil

I have read, discussed and understand the e safety rules and agree to follow these rules when:

- I use ICT (both in and out of school)
- I use my own equipment in school (when allowed) e.g. USBs, tablets etc.
- I use my own equipment out of school in a way that is related to me being a member of this school e.g. communicating with other members of the school, accessing school email, website etc.

Parent/Carer signature

We have discussed this and ……(child name) agrees to follow the e-Safety rules and to support the safe use of ICT at Holy Family Catholic Primary School.

Parent/Carer Signature: ……

Pupil Signature: ……

Class …… Date ……

Appendix 3

Parent/Carer Acceptable Use Policy Agreement

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

This Acceptable Use Policy is intended to ensure:

- That young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- That school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- That parents and carers are aware of the importance of e-safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

The school will try to ensure that pupils will have good access to ICT to enhance their learning and will, in return, expect the pupils to agree to be responsible users. A copy of the Pupil Acceptable Use Policy is attached to this permission form, so that parents / carers will be aware of the school expectations of the young people in their care.

Parents are requested to sign the permission form below to show their support of the school in this important aspect of the school's work.

Permission Form

As the parent/carer of the above pupil(s), I give permission for my son/daughter to have access to the internet and to ICT systems at school.

I know that my son/daughter has signed an Acceptable Use Agreement and has received, or will receive, e-safety education to help them understand the importance of safe use of ICT – both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my son's / daughter's activity on the ICT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's e-safety.

Pupil Name	
Parent/Carers Name	
Signed	
Date	

Appendix 4

Use of Digital/Video Images

The use of digital / video images plays an important part in learning activities. Pupils and members of staff may use digital photographs or videos to record evidence of activities in lessons and out of school. These images may then be used in presentations in subsequent lessons.

Images may also be used to celebrate success through their publication in newsletters, on the school website or twitter account and occasionally in the public media.

The school will comply with the Data Protection Act and request parents / carers permission before taking images of members of the school. We will also ensure that when images are published that the young people can not be identified by the use of their names.

Parents are requested to sign the permission form below to allow the school to take and use images of their children.

Permission Form

As the parent/carer of the above pupil, I agree to the school taking and using digital/video images of my child/children. I understand that the images will only be used to support learning activities or in publicity that reasonably celebrates success and promotes the work of the school.

I agree that if I take digital or video images at, or of, – school events which include images of children, other than my own, I will abide by these guidelines in my use of these images.

Pupil Name	
Parent/Carers Name	
Signed	
Date	

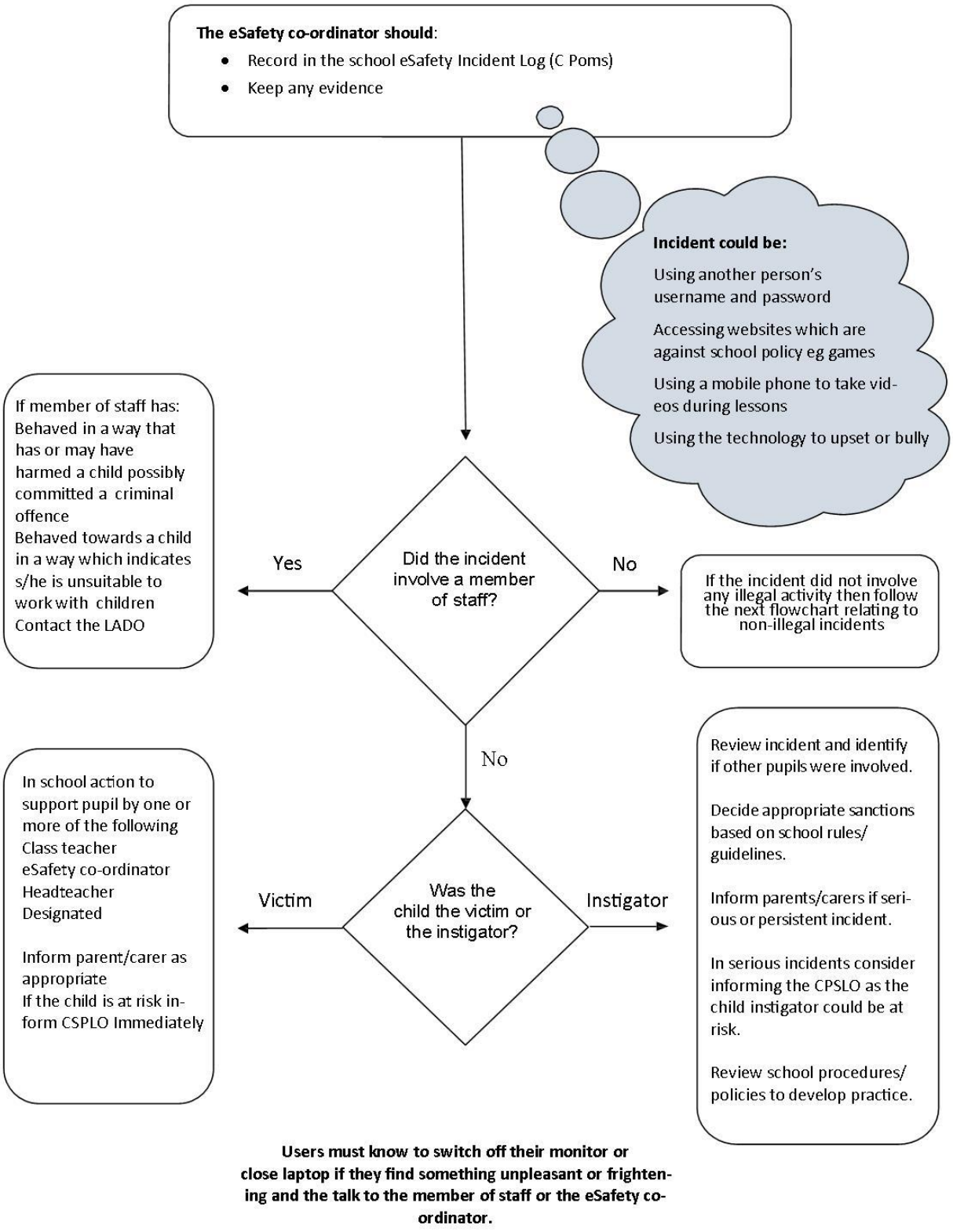
Student / Pupil Acceptable Use Agreement

On the following pages we have copied, for the information of parents and carers, Pupil Acceptable Use Agreement.

Appendix 5

Flowchart for Managing an e-Safety Incident

If the incident did not involve any illegal activity then follow this flowchart



Users must know to switch off their monitor or close laptop if they find something unpleasant or frightening and the talk to the member of staff or the eSafety co-ordinator.

Appendix 6


Childnet International
www.childnet.com
Be smart on the internet
S
SAFE
Keep safe by being careful not to give out personal information – such as your full name, email address, phone number, home address, photos or school name – to people you are chatting with online.
m
MEETING
Meeting someone you have only been in touch with online can be dangerous. Only do so with your parents' or carers' permission and even then only when they can be present.
a
ACCEPTING
Accepting emails, IM messages, or opening files, pictures or texts from people you don't know or trust can lead to problems – they may contain viruses or nasty messages!
r
RELIABLE
Information you find on the internet may not be true, or someone online may be lying about who they are.
t
TELL
Tell your parent, carer or a trusted adult if someone or something makes you feel uncomfortable or worried, or if you or someone you know is being bullied online.
You can report online abuse to the police at www.thinkuknow.co.uk
THINK U KNOW
www.kidsmart.org.uk
KidSMART
Visit Childnet's Kidsmart website to play interactive games and test your online safety knowledge. You can also share your favourite websites and online safety tips by Joining Hands with people all around the world.

Appendix 7

Current Legislation

Acts relating to monitoring of staff email

Data Protection Act 2018
The Act requires anyone who handles personal information to comply with important data protection principles when treating personal data relating to any living individual. The Act grants individuals rights of access to their personal data, compensation and prevention of processing.
http://www.hmso.gov.uk/acts/acts1998/19980029.htm

The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 http://www.hmso.gov.uk/si/si2000/20002699.htm

Regulation of Investigatory Powers Act 2000
Regulating the interception of communications and making it an offence to intercept or monitor communications without the consent of the parties involved in the communication. The RIP was enacted to comply with the Human Rights Act 1998. The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, however, permit a degree of monitoring and record keeping, for example, to ensure communications are relevant to school activity or to investigate or detect unauthorised use of the network. Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored. Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation.
http://www.hmso.gov.uk/acts/acts2000/20000023.htm

Human Rights Act 1998
http://www.hmso.gov.uk/acts/acts1998/19980042.htm

Other Acts relating to e-Safety

Racial and Religious Hatred Act 2006
It is a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Sexual Offences Act 2003
The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust.
Schools should already have a copy of "Children & Families: Safer from Sexual Crime" document as part of their child protection packs.
For more information www.teachernet.gov.uk

Communications Act 2003 (section 127)
Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence

liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

The Computer Misuse Act 1990 (sections 1–3)

Regardless of an individual's motivation, the Act makes it a criminal offence to gain:

- Access to computer files or software without permission (for example using another persons password to access files)
- Unauthorised access, as above, in order to commit a further criminal act (such as fraud)
- Impair the operation of a computer or program

UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences.

Malicious Communications Act 1988 (section 1)

This legislation makes it a criminal offence to send an electronic message (e-mail) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety.

Copyright, Design and Patents Act 1988

Copyright is the right to prevent others from copying or using work without permission. Works such as text, music, sound, film and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer. Copyright infringement is to copy all or a substantial part of anyone's work without obtaining them author's permission. Usually a license associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a license before you copy or use someone else's material. It is also illegal to adapt or use software without a license or in ways prohibited by the terms of the software license.

Public Order Act 1986 (sections 17 – 29)

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

Protection of Children Act 1978 (Section 1)

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.

Obscene Publications Act 1959 and 1964

Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other.
A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Keeping Children Safe in Education September 2020

The use of technology has become a significant component of many safeguarding issues. Child sexual exploitation; radicalisation; sexual predation: technology often provides the platform that facilitates harm. An effective approach to online safety empowers a school or college to protect and educate the whole school or college community in their use of technology and establishes mechanisms to identify, intervene in, and escalate any incident where appropriate.

The breadth of issues classified within online safety is considerable, but can be categorised into three areas of risk:

- Content: being exposed to illegal, inappropriate or harmful material; for example pornography, fake news, racist or radical and extremist views;
- Contact: being subjected to harmful online interaction with other users; for example commercial advertising as well as adults posing as children or young adults;
- Conduct: personal online behaviour that increases the likelihood of, or causes, harm; for example making, sending and receiving explicit images, or online bullying.

Protecting children

Governing bodies and proprietors should be doing all that they reasonably can to limit children's exposure to the above risks from the school's or college's IT system. As part of this process, governing bodies and proprietors should ensure their school or college has appropriate filters and monitoring systems in place.

Whilst considering their responsibility to safeguard and promote the welfare of children, and provide them with a safe environment in which to learn, governing bodies and proprietors should consider the age range of their pupils, the number of pupils, how often they access the IT system and the proportionality of costs vs risks.

The appropriateness of any filters and monitoring systems are a matter for individual schools and colleges and will be informed in part, by the risk assessment required by the Prevent Duty.119 The UK Safer Internet Centre has published guidance as to what "appropriate" filtering and monitoring might look like: UK Safer Internet Centre: appropriate filtering and monitoring.

Guidance on e-security is available from the National Education Network. Support for schools is available via the: schools' buying strategy with specific advice on procurement here: buying for schools.

Whilst filtering and monitoring is an important part of the online safety picture for schools and colleges to consider, it is only one part. Governors and proprietors should consider a whole school or college approach to online safety. This will include a clear policy on the use of mobile technology in the school or college. Many children have unlimited and unrestricted access to the internet via 3G, 4G and 5G in particular and the school and college should carefully consider how this is managed on their premises.

Whilst it is essential that governing bodies and proprietors ensure that appropriate filters and monitoring systems are in place, they should be careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regard to online teaching and safeguarding.

Appendix 8

Communication

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks / disadvantages:

	Staff & other adults				Pupils			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school	x						x	
Use of mobile phones in lessons		x						x
Use of mobile phones in social time	x							x
Taking photos on mobile phones or other camera devices		x						x
Use of hand held devices e.g. Tablets	x						x	
Use of personal email addresses in school, or on school network				x				x
Use of school email for personal emails				x				x
Use of chat rooms / facilities		x					x	
Use of instant messaging		x					x	
Use of social networking sites in school other than VLE				x				x
Use of blogs	x				x			

Appropriate and Inappropriate Behaviour

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other ICT systems. Other activities e.g. Cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities. The school policy restricts certain internet usage as follows:

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	child sexual abuse images					x
	promotion or conduct of illegal acts, e.g. under the child protection, obscenity, computer misuse and fraud legislation					x
	adult material that potentially breaches the Obscene Publications Act in the UK					x
	criminally racist material in UK					x
	pornography				x	
	promotion of any kind of discrimination				x	
	promotion of racial or religious hatred				x	
	threatening behaviour, including promotion of physical violence or mental harm				x	
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				x	
Using school systems to run a private business					x	
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school				x		
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions						x
Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)					x	
Creating or intentionally propagating computer viruses or other harmful files					x	
Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet					x	
On-line gaming (educational)		x				
On-line gaming (non educational)			x			
On-line gambling					x	
On-line shopping / commerce					x	
File sharing		x				
Use of social networking sites				x		
Use of video broadcasting e.g. YouTube				x		

Responding to Incidents of Misuse

Pupils — Actions

Incidents:	Refer to class teacher	Refer to SLT	Refer to Head teacher	Refer to Police	Refer to ICT Co-ordinator action re	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction e.g. detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal.			x						
Unauthorised use of non-educational sites during lessons					x			x	
Unauthorised use of mobile phone / digital camera / other handheld device	x								
Unauthorised use of social networking / instant messaging / personal email					x				
Unauthorised downloading or uploading of files					x				
Allowing others to access school network by sharing username and passwords	x							x	
Attempting to access or accessing the school network, using another pupil's / pupil's account		x							
Attempting to access or accessing the school network, using the account of a member of staff					x				
Corrupting or destroying the data of other users		x							
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature		x				x		x	
Continued infringements of the above, following previous warnings or sanctions			x			x	x		
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school			x						
Using proxy sites or other means to subvert the school's filtering system		x			x				
Accidentally accessing offensive or pornographic material and failing to report the incident		x							
Deliberately accessing or trying to access offensive or pornographic material			x						
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act		x							

It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse:

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

- child sexual abuse images
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials

The head teacher should be consulted with the evidence of the activity. If the evidence confirms the misuse the head teacher has a duty to report the incident to the police.

Staff Actions

Incidents:	Refer to line	Refer to Head	Refer to Local	Refer to Police	Refer to ICT Co-	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal.		x		x				x
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email	x							
Unauthorised downloading or uploading of files					x			
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	x							
Careless use of personal data e.g. holding or transferring data in an insecure manner		x						
Deliberate actions to breach data protection or network security rules					x			
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		x			x			
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature					x			
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with pupils.	x				x			
Actions which could compromise the staff member's professional standing		x						
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		x						
Using proxy sites or other means to subvert the school's filtering system					x			
Accidentally accessing offensive or pornographic material and failing to report the incident					x			
Deliberately accessing or trying to access offensive or pornographic material		x						
Breaching copyright or licensing regulations	x							
Continued infringements of the above, following previous warnings or sanctions		x						

Glossary of terms

AUP	Acceptable Use Policy
CEOP	Child Exploitation and Online Protection Centre (part of UK Police dedicated to protecting children from sexual abuse) providers of the Think U Know programmes.
CPD	Continuous Professional Development
CYPS	Children and Young Peoples Services (in Local Authorities)
DCSF	Department for Children, Schools and Families
ECM	Every Child Matters
FOSI	Family Online Safety Institute
HSTF	Home Secretary's Task Force on Child Protection on the Internet
ICO	Information Commissioners Office
ICT	Information and Communications Technology
INSET	In Service Education and Training
IP address	The label that identifies each computer to other computers using the IP (internet protocol)
ISP	Internet Service Provider
ISPA	Internet Service Providers' Association
IWF	Internet Watch Foundation
KS1.	Key Stage 1 / 2 – primary schools are structured within these multiple age groups
LA	Local Authority
LAN	Local Area Network
Learning Platform	A learning platform brings together hardware, software and supporting services to support teaching, learning, management and administration.
LSCB	Local Safeguarding Children Board
MIS	Management Information System
MLE	Managed Learning Environment
Ofcom	Office of Communications (Independent communications sector regulator)
Ofsted	Office for Standards in Education, Children's Services and Skills
PHSE	Personal, Health and Social Education
SEF	Self Evaluation Form – used by schools for self evaluation and reviewed by Ofsted prior to visiting schools for an inspection
SRF	Self Review Form – a tool used by schools to evaluate the quality of their ICT provision.
Tablet	A handheld, portable device operating web-connected content of downloaded/inbuilts apps
TUK	Think U Know – educational e-safety programmes for schools, young people and parents.
VLE	Virtual Learning Environment – an online software system designed to support teaching and learning in school and beyond.
WAP	Wireless Application Protocol