'Online Safety Policy'

Updated	Jan 2019
Reviewed	Oct 2022
Next Review	Oct 2022

With God's help we
CARE - BUILD - FOLLOW - THINK

In accordance with our vision and mission - with God's help we, **care, build, follow and think** lies at the heart of this policy. We believe that all people are made in the image of God and are unconditionally loved by God. Everyone is equal and we treat each other with dignity and respect. Our school is a place where everyone is able to flourish in a loving and hospitable community.

INTRODUCTION:

This policy applies to all staff, pupils, governors and visitors accessing the Internet or using technological devices on school premises. This includes staff or pupil use of personal devices such as mobile phones or ipads, which are brought into school. This policy is also applicable where staff have been provided with school issued devices for use off site such as laptop or mobile phone.

The use of information and communication technology is an integral part of the National Curriculum (NC) and is a key skill for everyday life. Computers, I-pads, programmable robots, and video cameras are a few of the tools that we use to acquire, organise, store, interpret and communicate and present information. We recognise that pupils are entitled to quality hardware and software and a structured and progressive approach to learning the skills that are needed. Whilst technology has many benefits, we recognise that clear procedures for appropriate use and education, for staff as well as students, about online behaviours, age restrictions and potential risks is crucial.

AIM:

- To educate staff, pupils and parents about the pros and cons of using new technology both within, and outside of, the school environment;
- To develop links with parents/carers and the wider community to show awareness of the benefits and potential issues related to technology;
- To teach the children how to use the internet safely;
- To show what procedures the school have in place to safeguard and protect children using the Internet.

Why is Internet use important and what are the benefits to the school?

- It gives pupils immediate access to a rich source of materials;
- It means they can present information in new ways, which helps pupils understand and use it more readily;
- It can motivate and enthuse pupils;
- It has the flexibility to meet the individual needs and abilities of each pupil;
- It offers the potential for effective group working;
- It is a part of the statutory curriculum;
- It enhances the school's management information and business administration systems;
- Information and cultural exchanges can be made between pupils world wide;
- It allows for discussion with experts in many fields for pupils and staff;
- It enables staff professional development- access to educational materials and good curriculum practice.

How will Internet use enhance learning?

- Pupils will be taught what internet use is acceptable and what is not and be given clear rules to adhere to;
- Pupils will also be educated in taking responsibility for what Internet they access;
- Staff will select sites which will support the learning outcomes planned for pupils' age and maturity;
- Older children will be taught how to find appropriate sites to support their research and learning
- Internet access will be planned to enrich and extend learning activities.

How will pupils be taught to assess Internet content?

- Pupils will be taught ways to validate information before accepting its accuracy;
- Pupils will be taught to acknowledge the source of information, when using Internet material for their own use;
- Pupils will be made aware that the writer of an email or the author of a web page might not be the person they claim to be;
- Pupils will be encouraged to tell a teacher immediately if they encounter any material that they feel is inappropriate or that makes them feel uncomfortable;
- Pupils will be taught to recognise and deal with SPAM mail.

How will the Internet be managed?

E-mail

- Pupils must only use approved e-mail accounts on the school system for educational purposes;
- Pupils will not be allowed to access personal e-mail accounts from the school system;
- Pupils may send e-mails as part of planned lessons but will not be given an individual e-mail account;
- Pupils must not reveal personal information about themselves or others in e-mail communication or arrange to meet up with anyone;
- Pupils must tell a teacher if they receive any offensive e-mails;
- An e-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper;
- The school provides all staff with a professional email account to use for all school related business;
- All emails, should be professional in tone and checked carefully before sending;
- Staff should inform the IT co-ordinator or head teacher if they receive an offensive or inappropriate e-mail via the school system.
- All staff to include disclaimer at the bottom of all emails from professional account

Authorising Internet access

- At Key Stage 1, the majority of access to the Internet will be by teacher or adult demonstration. However there may be situations where children have supervised access to specific approved online materials. The use of child friendly applications such as 'youtube for kids' and 'swiggle' will also be encouraged;
- At Key Stage 2, Internet access will be granted to a whole class as part of a scheme of work after a suitable education in responsible Internet use;
- Parents must sign the home, school agreement stating they will support the school in teaching of using the internet safety
- Children will also be asked to sign a permission form to say that they will adhere to the rules of using the Internet safely and for its intended use using the home school agreement;
- Children who are using the Internet will be appropriately supervised.

Published content and the school website

- The contact details on the website are the school address and telephone number as well as the head teacher's email address. Staff or pupil's personal information will not be published;
- Written permission from parents/carers is be obtained before photographs or names are published onto the school website. Each class teacher is given a list of children whose name or photograph is not permitted onto the school website.

Social networking and personal publishing

- The school will block/filter social networking sites;
- Pupils will be taught what sites are appropriate for their age group and the dangers of using social media websites and gaming websites with an age restriction;
- Parents will be advised that the use of social networking is inappropriate for primary aged pupils.

Filtering

- Internet access is purchased from a supplier that provides a service designed for pupils. This includes filtering appropriate to the age of the pupils;
- The IT technician will ensure regular checks are made to ensure that filtering methods are effective;
- If staff or pupils discover an unsuitable site, it must be reported to the IT co-ordinator lead who will then record it in Appendix 6 and report to the IT technician;
- Emails will be filtered and accessed through the Schools Broadband to provide security and protection for the children;
- All users have unique usernames to access the school network, this ensures that they receive the appropriate level of filtering;
- Virus protection will be reviewed and updated regularly.

Managing emerging technologies

- Emerging technologies will be examined by adults for educational benefit and assessed before use in school is allowed;
- Mobile phones will not be used in lessons or formal school time. They will be handed to the class teacher at the start of the school day and returned before home time. Throughout the day, mobile phones should be locked away where only the adult in charge can have access to them;
- Staff mobile phones are permitted onto school grounds although it is the responsibility of the staff member to ensure that there is no inappropriate content stored on their device when brought onto school grounds.

What are the risks of using the Internet and how will this be dealt with?

Assessing risks

- In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. The school will supervise pupils and take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of information available via the Internet, it is not possible to guarantee that unsuitable material will never appear on a terminal. Neither the school accept liability for the material accessed, or any consequences thereof;
- The use of computer systems without permission or for purposes not agreed by the school could constitute a criminal offence under the Computer Misuse Act 1990;
- The Head teacher will ensure that the policy is implemented effectively.

Maintenance of the school's security system

- Security strategies will be discussed with PDET;
- The IT technician will ensure that the system has the capacity to take increased traffic caused by Internet use;
- The security of the whole system will be reviewed by the IT technician with regard to threats to security from Internet access;
- Virus protection will be installed and updated regularly;

Misuse of the Internet

- In the event of minor or accidental misuse, internal investigations should be initiated and procedures should follow appropriately using the flow chart on page 11;
- All security breaches, lost/stolen equipment or data, or misuse of the Internet should be reported immediately to the head teacher, who will log the information on to 'My Concern' and follow the necessary procedures;
- Responsibility for handling incidents will be given to the Head Teacher;
- Any complaint about staff misuse must be referred to the Head teacher;
- Sanctions may involve being interviewed or receive counselling by the Head Teacher, and, if appropriate, informing parents and carers;
- Parents and pupils will need to work in partnership with staff to resolve issues;
- A pupil may have internet or computer access denied for a period of time depending on the nature of the incident;

- If there are any occasions when the police must be contacted, early contact will be made to establish legalities and to discuss strategies to move forward;
- Complaints of a Child Protection nature are dealt with in accordance with the School's Child Protection Procedures.

Introducing the Internet-safety policy to staff, pupils and parents

- Internet-safety rules will be posted in all networking areas and discussed with pupils at the start of each term;
- Pupils will be informed that their Internet use will be monitored;
- Pupils are encouraged to report any material they find distasteful, uncomfortable or threatening to their class teacher;
- All staff members will be provided with the Internet-safety policy, have its importance explained
- Staff will be kept up to date by the IT co-ordinator with any new changes to the policy and any changes linked to internet-safety in schools;
- Staff will be educated about new technology and any implications they have in school through staff meetings;
- Parents' attention will be drawn to the policy through the use of the school's website and when opportunities arise for outside agencies to talk to parents;
- Pupils will be taught to adopt safe and responsible practices when using new technology through PSHE, IT lessons and an age appropriate curriculum alongside the assistance of outside agencies;
- If a pupil has a specific learning requirement, or poor social understanding, careful consideration is given to the planning and delivery of internet-safety awareness and Internet access.

Responsibilities

IT Technical staff must ensure that:

- The school's infrastructure is secure and not open to misuse;
- The anti-virus software is installed and maintained on all school machines;
- The school's filtering policy is applied and updated on a regular basis
- They keep up to date with internet-safety technical information in order to maintain the security of the schools network and to safeguard pupils;
- Staff are kept up to date with any new changes with regards to internet-safety in school;

Children must ensure that:

- They read and sign the document Rules for Responsible Use (Appendix 2 and 3) and abide by the appropriate rules set out in the document;
- They use the internet and technology in a safe and responsible manner within school, which shall be taught and reinforced by class teachers;
- They inform staff of any inappropriate material or cyber bullying they come into contact with. Staff
- Staff members should then record this onto 'My Concern'

Parents must ensure that

- They read the Acceptable Use Rules on an annual basis or first time entry to the school. They must also sign that they will support the rules in the home-school agreement.

- They try to attend any internet-safety sessions that are run to increase their knowledge of key Internet safety issues;
- They encourage their child/children to talk about what they have been doing on the Internet and to discuss any issues that they may find upsetting.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate students / pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.

- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other *students / pupils* in the digital / video images.

- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.

- Care should be taken when taking digital / video images that students / pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.

- Students / pupils must not take, use, share, publish or distribute images of others without their permission

- Photographs published on the website, or elsewhere that include students / pupils will be selected carefully and will comply with good practice guidance on the use of such images.

- Students' / Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.

- Written permission from parents or carers will be obtained before photographs of students / pupils are published on the school website, when children first start at the school

- Student's / Pupil's work can only be published with the permission of the student / pupil and parents or carers.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

The school / academy must ensure that:

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing".
- It has a Data Protection Policy
- It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)
- Responsible persons are appointed / identified - Senior Information Risk Officer (SIRO) and Information Asset Owners (IAOs)
- Risk assessments are carried out
- It has clear and understood arrangements for the security, storage and transfer of personal data
- Data subjects have rights of access and there are clear procedures for this to be obtained
- There are clear and understood policies and routines for the deletion and disposal of data
- There is a policy for reporting, logging, managing and recovering from information risk incidents
- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties
- There are clear policies about the use of cloud storage / cloud computing which ensure that such data storage meets the requirements laid down by the Information Commissioner's Office.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.

When personal data is stored on any portable computer system, memory stick or any other removable media:

- the data must be encrypted and password protected
- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete

Communications

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				Students / 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 / cameras				x				x
Use of other mobile devices eg tablets, gaming devices	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 messaging apps		x			x			
Use of social media		x			x			
Use of blogs	x				x			

The school may also wish to add some of the following policy statements about the use of communications technologies, in place of, or in addition to the above table:

When using communication technologies the school considers the following as good practice:

- **The official *school* email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored.**
- **Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.** (SWGfL BOOST includes an anonymous reporting app Whisper - http://www.swgfl.org.uk/Staying-Safe/E-Safety-BOOST/Boost-landing-page/Boost-Hub/SWGfL-Whisper**)**
- **Any digital communication between staff and students / pupils or parents / carers (email, chat, VLE etc) must be professional in tone and content.** *These communications may only take place on official (monitored) school / academy systems. Personal email addresses, text messaging or social media must not be used for these communications.*
- *Whole class / group email addresses may be used at KS1, while students / pupils at KS2 and above will be provided with individual school / academy email addresses for educational use.* (Schools / academies may choose to use group or class email addresses for younger age groups eg. at KS1)
- *Students / pupils should be taught about e-safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.*
- *Personal information should not be posted on the school / academy website and only official email addresses should be used to identify members of staff.*

Social Media - Protecting Professional Identity

All schools, academies and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools/academies and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the *school or* local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through limiting access to personal information:

- Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions

- Risk assessment, including legal risk

School staff should ensure that:

- No reference should be made in social media to pupils, parents / carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the *school* or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

The *school's* use of social media for professional purposes will be checked regularly by the senior risk officer and e-safety committee to ensure compliance with the Social Media, Data Protection, Communications, Digital Image and Video Policies.

Unsuitable / inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school / academy and all other technical 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 believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts usage as follows:

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	**Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978**					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	pornography				X	
	promotion of any kind of discrimination				X	

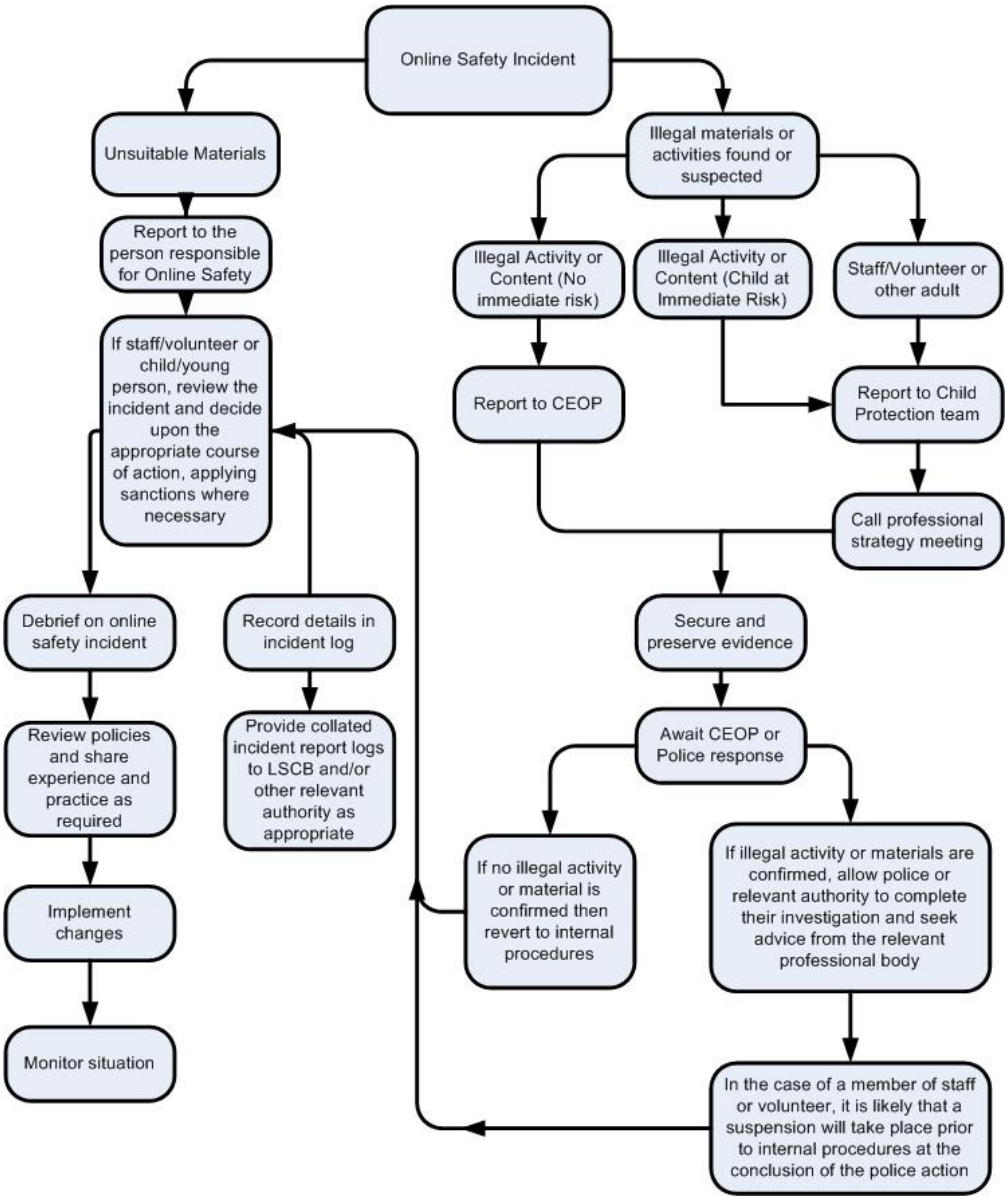
	threatening behaviour, including promotion of physical violence or mental harm				X	
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Using school systems to run a private business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / academy					X	
Infringing copyright					X	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)					X	
Creating or propagating computer viruses or other harmful files					X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)					X	
On-line gaming (educational)	x					
On-line gaming (non educational)		x				
On-line gambling				x		
On-line shopping / commerce			x			
File sharing			x			
Use of social media		x				
Use of messaging apps			x			
Use of video broadcasting eg Youtube			x			

(The *school / academy* should agree its own responses and place the ticks in the relevant columns, in the table above. They may also wish to add additional text to the column(s) on the left to clarify issues. The last section of the table has been left blank for *schools / academies* to decide their own responses)

Responding to incidents of misuse
This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see “User Actions” above).

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the police.



Other Incidents

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

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff / volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the url of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:

- Internal response or discipline procedures
- Involvement by Local Authority or national / local organisation (as relevant).
- Police involvement and/or action

- **If content being reviewed includes images of Child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:**
  - incidents of 'grooming' behaviour
  - the sending of obscene materials to a child
  - adult material which potentially breaches the Obscene Publications Act
  - criminally racist material
  - other criminal conduct, activity or materials
- **Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.**

It is important that all of the above steps are taken as they will provide an evidence trail for the *school / academy* and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the group for evidence and reference purposes.

Appendix 1

Cottingham CE Primary School

Acceptable Internet Use Statement for Staff

The computer system is owned by the school and is made available to students to further their learning and to staff to enhance their professional activities including teaching, research, administration and management.

The school reserves the right to examine or delete any files that may be held on its computer system or to monitor any Internet sites visited.

Staff requesting Internet access should sign a copy of the Acceptable Internet Use Statement and return it to the ICT Co-ordinator.

Activity that threatens the integrity of the school ICT systems, or activity that attacks or corrupts other systems, is forbidden;

Users are responsible for all e-mails sent and for contacts made that may result in e-mails being received;

Posting anonymous messages and forwarding chain letters is forbidden;
Copyright of materials must be respected;

All Internet activity should be appropriate to staff professional activity or the student's education. Legitimate private interests may be followed where these cause no difficulties for other users and do not compromise school use;

The same professional levels of language and content should be applied as for letters or other media, particularly as e-mails are often forwarded or may be sent inadvertently to the wrong person;
Use for personal financial gain, gambling, political purposes or advertising is forbidden;

Users must access only those sites and materials relevant to their work in school. Users will be aware when they are accessing inappropriate materials and should expect to have their permission to use the system removed.

Full name …. … … … … … … … … … Post … … … … … … … … … …
Signed … … … … … … … Date … … … … … …
Access granted … … … … … … … Date … … … … … …

Appendix 2

KS1 pupils e-safety agreement

Keeping me safe at home and at school

We check with a grown up before using the internet.

We tell a grown up if something we see makes us feel worried.

If we get stuck or lost on the internet we will ask for help.

We can write polite and friendly messages to people we know.

We will keep our personal information, our name, address, our school, our pictures "Top Secret" and not share on the internet.

We will not bring mobile phones or other electronic devices (e.g. tablets, ipods, games consoles) to school.

Signed/Name:

Class:

Appendix 3

Cottingham CE Primary School

KS2 Pupils' Rules for Responsible Internet Use

The school has installed computers and Internet access to help our learning. These rules will keep everyone safe and help us be fair to others.

I will not access other people's files;

I will only use the computers for school work and homework;

I will ask permission from a member of staff before using the Internet;

I will only e-mail people whom I know, or my teacher has approved;

The messages I send will be polite and sensible;

I will not reveal any information about myself or others;

To help protect other pupils and myself, I will tell a teacher if I see anything I am unhappy with or I receive messages I do not like;

I understand that the school may check my computer files and may monitor the Internet sites I visit.

Signed:

Class:

Appendix 4

Parents information regarding internet usage at school

Dear Parents

Responsible Use of the Internet

As part of pupils' curriculum enhancement and the development of computing skills, Cottingham CE Primary provides supervised access to the Internet, sometimes including e-mail. The use of information and communication technology is an integral part of the National Curriculum (NC) and is a key skill for everyday life. Computers, Ipads, programmable robots, and video cameras are a few of the tools that we use to acquire, organise, store, interpret and communicate and present information. We recognise that pupils are entitled to quality hardware and software and a structured and progressive approach to learning the skills that are needed. Whilst technology has many benefits, we recognise that clear procedures for appropriate use and education about online behaviours, age restrictions and potential risks is crucial.

Our school Internet access provider operates a filtering system that restricts access to inappropriate materials.

Whilst every endeavour is made to ensure that suitable restrictions are placed on the ability of children to access inappropriate materials, we cannot be held responsible for the nature or content of materials accessed through the Internet. NCC will not be liable under any circumstances for any damages arising from your child’s use of the Internet facilities. I enclose a copy of the Rules for Responsible Internet Use that we operate at Cottingham. Should you wish to discuss any aspect of Internet use, please telephone me to arrange an appointment.

Yours Sincerely

Emma Hurn (*Computing lead)*

Appendix 5

References

Particularly for Parents:

Government site for Parents Information about education for parents www.dfee.gov.uk/parents

NCH Action for Children. A Parents'Guide to the Internet leaflet. www.nchafc.org.uk/internet

Parents and IT. BECTa information sheet. www.becta.org.uk/info-sheets/parents.html

Parents' Information Network(PIN).Guidelines on using the Internet safely. www.pin-parents.com

Superhighway Safety Pack http://vtc.ngfl.gov.uk/vtc/library/safety.html

Free pack from DfEE on safe Internet use Tel: 0845 6022260

Particularly for Schools:

Association for Co-ordinators and Teachers of IT (ACITT. Acceptable Use Policy for UK Schools.www.acitt.org.uk/aup.html

Connecting Schools, Networking People 2000

BECTa, October 1999 (free order line) Tel: 024 7641 6669

Kent NGfL Website. Latest version of this policy.

www.kent.gov.uk/ngfl/policy.html

Internet Watch Foundation www.iwf.org.ukReporting

Illegal Internet material Tel: 0845 600 8844.

Irish National Centre for Technology in Education. Comprehensive advice on Internet use www.ncte.ie/support.htm

Promoting the Responsible Use of the Internet in Schools. British Computer Society / NAACE www.bcs.org.uk/iap.htm

The Internet and the World Wide Web. Information sheet published April '99 www.becta.org.uk/infosheets/internet.html

With God's help we
CARE - BUILD - FOLLOW - THINK