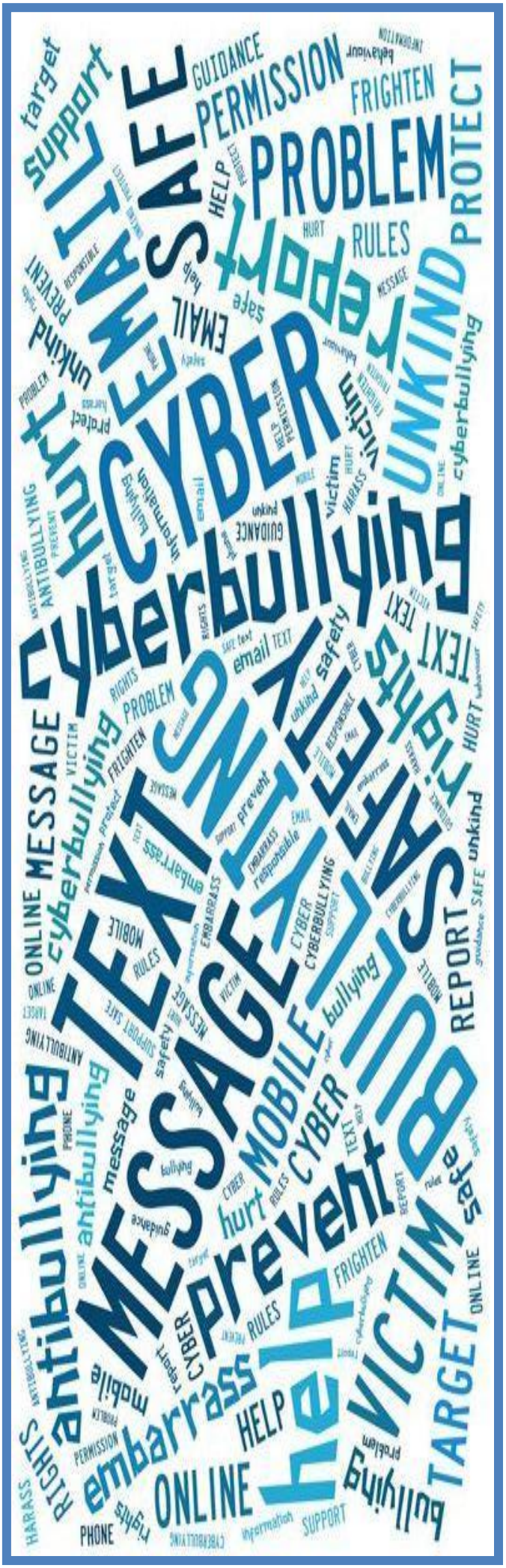


E-Safety & Anti-cyberbullying Policy

Related Policies:

Behaviour Policy

Anti-bullying Policy

Safeguarding Policy

Equality Policy

ICT Policy

SUMMER 2015

woodstock
CE PRIMARY SCHOOL

E-Safety Policy

CONTENTS

1. Our Vision

We are living in an increasingly connected world where, alongside the benefits of access to technology, come increased risks to children. Lack of guidance and learning in E-safety can mean children are unaware of the unintended consequences of their on-line behaviour or actions. It highlights the need to educate pupils and the school community about the benefits and risks of using Internet technologies and electronic communications, and provide safeguards and awareness for users, to enable them to control their online experience.

'Our vision is to make the children at Woodstock School as safe and productive in the on-line world, both in school and outside of school, as they are in the real world with particular focus on protection against grooming, cyberbullying and becoming a positive e-citizen.'

Our policy and practice against this is clearly articulated in this E-Safety Policy.

2. What is E-safety?

E-safety is a school's ability to **protect and educate** a schools pupils and staff in their use of technology as well as having appropriate mechanisms in place to **respond** to, and support any incident where appropriate.

a. Protect

Protecting pupils means providing a safe learning environment by using appropriate monitoring and filtering to control what children can access while at school. But, this only protects them while they are on school premises. Education around e-safety is the only way to ensure that, wherever they are, they know how to stay safe online.

b. Educate

Learning about e-safety is a vital life skill. Empowering children at an early age with the knowledge to safeguard themselves and their personal information is something that needs to be nurtured throughout school to see them into adult life. Equally it is important to empower adults, particularly parents, with the right information so that they can identify risky behaviour, or mitigate the possibility of risk.

The School's E-safety curriculum is progressive and covers a wide range of aspects, including:

- Online behaviour – understanding what constitutes cyber-bullying, inappropriate content and sexting, how to behave safely and with respect for others.
- Protecting your online reputation – understanding both the risks and rewards of sharing personal information online (your digital footprint).
- Learning to evaluate internet content – understanding how to research, evaluate and use published material

c. Respond

Responding to issues is both about ensuring pupils know what to do if anything happens to put their online safety at risk, and taking direct and immediate action as a school where incidents occur.

Woodstock CE Primary School has clear and robust policies and procedures to identify and immediately respond to e-safety risks or incidents, efficiently and consistently. It is important to note that the school's remit to act goes

beyond the classroom, to regulate pupils' conduct and safeguard them when they are not on school premises or under the lawful charge of school staff.

3. Why use the internet for Teaching and Learning?

A number of studies and government projects have identified the benefits to be gained through the appropriate use of the Internet.

The rapid developments in electronic communications are having many effects on society. Only ten years ago we were asking whether the Internet should be used in all schools. Now, it is an essential aspect of learning across all walks of life. In school, access to the internet is essential to:

- Raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the School's management functions.
- Prepare children and young people for life in 21st century in terms for education, business and social interaction. The school has a duty to provide pupils with quality Internet access as part of their learning experience.
- Teach pupils how to evaluate Internet information and to take care of their own safety and security rather than be sheltered from potential risks.

There are many benefits of the Internet to learning:

- Access to world-wide educational resources
- Collaboration and communication between pupils
- Access to anytime, anywhere learning
- Educational and cultural exchanges between pupils world-wide to develop global understanding
- Access to experts in many fields for pupils and staff
- Professional development for staff through access to national developments, educational materials and example of effective curriculum practice
- Collaboration across support services and professional associations
- Improved access to technical support including remote management of networks and automatic system updates
- Exchange of information

With increased use of the Internet, protecting and educating pupils to manage the risk becomes our primary concern. As a school we commit to provide parents with support and information in keeping children safe online.

4. Who does this policy cover?

There are multiple groups that are impacted by this Policy. They are:

- Pupils
- Staff
- Parents
- School Governing Body

a. Pupils

A pupil's perceptions of risks will vary; the school has a clear Code of Conduct for Responsible Use of Technology which is developed and agreed by staff and pupils together. To support appropriate access to the Internet and use of electronic communications, we ensure that:

- The E-safety Policy is summarised to, and discussed with our Children's Council and their comments invited.
- The E-safety Responsible Use Policy is shared with pupils, and parents are encouraged to discuss and emphasise the Policy for home use.
- The E-safety Code of Conduct is clearly posted in all networked rooms.
- Pupils are frequently informed that Internet use is monitored.
- A professionally led E-safety training programme is delivered to all pupils to raise the awareness and importance of safe and responsible use of the Internet and other electronic communications tools. This programme is delivered in the classroom through Computing skills lessons and PSHE sessions, and beyond the classroom through structured annual training and specially focussed assemblies. E-safety messages are re-enforced each time Internet access or ICT usage is given.

b. Staff and Volunteers

Woodstock CE Primary School E-safety Policy will only be effective if all staff, and support volunteers subscribe to its values and methods. As standard practice we ensure that:

- All staff are given the School E-safety Policy and its application and importance explained.
- Staff & volunteers are asked to read and sign in agreement to the 'Staff Acceptable Use Policy'
- Staff are fully aware that Internet traffic can and will be monitored and traced to the individual user. Discretion and professional conduct is essential.
- The E-safety & Acceptable Use Policies are a core part of the induction programme for any new staff and volunteers.
- Training for teaching and non-teaching staff in safe and responsible Internet use and on the school E-safety Policy is provided regularly. Classroom practice is monitored periodically to ensure effective compliance.

c. Parents

Internet use in pupils' homes is increasing rapidly. Unless parents are aware of the dangers, pupils may have unintended unrestricted access to the Internet. As a school, we recognise the importance of striking a careful balance between informing and alarming parents. Our policy is to:

- Draw parents' attention to E-safety resources in particular the school's E-safety Policy, relevant articles and resources from trusted sources, and online reporting procedures in newsletters and on the school website.
- Handle internet issues sensitively, to inform parents without alarm.
- Encourage a partnership approach with parents where careful and informed practise can be supported in and out of school. This includes professionally delivered parent E-safety information evenings that build awareness of benefits and risks, and offer independent advice and best practice suggestions for safe home Internet and e-communications use.

d. School Governing Body

All Governors of the school are expected to understand, uphold and ensure e-safety best practice for staff and pupils. As Internet and communications access broadens, so governors must ensure that the school keeps pace in its policies and procedures and can effectively protect, educate and respond. To support this, we ensure:

- ICT and E-safety are a core part of our School Raising Achievement Plan. A nominated E-safety governor is responsible for ensuring effective practice and partnering progress towards agreed commitments and targets. Commitments and process are reviewed by the full Governing Body every term.
- All Governors receive professionally delivered E-safety training alongside staff and are clear as to their role in due diligence.
- All Governors receive an E-safety Report outlining implemented practices and reported incidents each term.
- Governors are able to play a role in extending our E-safety reach into the wider school community.

As a School we have formed an E-safety Committee which consists of members from all of these stakeholder groups as well as representation from external E-safety and ICT experts.

5. Policy

a. Cyber Bullying

Online bullying and harassment via Instant messaging, mobile phone texting, e-mail and chat rooms are potential problems that can have a serious effect on pupils both in and outside school. The methods and the audience are broader than traditional bullying and the perceived anonymity can make escalation and un-intended involvement an increased risk. Woodstock CE Primary School has a range of strategies and policies to prevent online bullying, outlined in various sections of this Policy. These include:

- No access to public chat-rooms, Instant Messaging services and bulletin boards.
- Pupils are taught how to use the Internet safely and responsibly, and are given access to guidance and support resources from a variety of sources. Specific education and training on cyber bullying (understanding what behaviour constitutes cyberbullying and its impact, how to handle concerns and report incidents) is given as part of an annual Anti-bullying Week and E-safety Day.
- Pupils are encouraged to discuss any concerns or worries they have about online bullying and harassment with staff, who have a range of materials available to support pupils and their families.
- Pupils are informed on how to report cyber bullying both directly within the platform they are on, and to school.
- Complaints of cyber bullying are dealt with in accordance with our Anti-bullying Policy.
- Complaints related to child protection are dealt with in accordance with school child protection procedures.

b. Grooming

Grooming is a word used to describe how people who want to co-opt or potentially harm children and young people get close to them, and often their families, and gain their trust. Online grooming may occur by people forming relationships with children and pretending to be their friend. They do this by finding out information and seeking to establish false trust. The school has measures in place to educate and protect pupils against this risk. These include:

- No access to public chat-rooms, Instant Messaging services and bulletin boards. No mobile phones.
- All online access and pupil generated content in school is monitored and password protected.
- Pupils are taught how to behave responsibly on line and the ‘golden rules’ in protecting personal information. More information is outlined in Section 7 of this Policy: Behaviours.
- Pupils, staff, parents and governors are provided with appropriately targeted training on risks and solutions to keep safe on line.

c. School Managed Content and Authorised Access

Woodstock CE Primary School has very clear measures and controls in place to enable responsible Internet access and usage. These are outlined as a key part of this E-safety Policy, as below:

Authorising Internet Use:

At Woodstock Primary School pupil usage is supervised, with access to specific approved online materials. Pupils are authorised to access the internet as a group or independently, depending on the activity. All staff must read and sign the 'Staff Acceptable Use Policy' before using any school ICT resource and parents are equally requested to share the Acceptable Use Policy with their children.

In order to be granted Internet access, pupils must complete the E-safety Code of Conduct for Responsible Use of Technology form. A list of children without permission to use the Internet is kept in the school office and is known to teaching staff.

Managing Filtering:

Whilst levels of Internet access and supervision will vary according to the pupils' age and experience, our policy is that Internet access must be appropriate for all members of the school community. Our Internet connection was arranged by IT support company 123 ICT following advice from Oxfordshire County Council and provision is through Schools Broadband, a specialist division of Talk Straight Ltd, a leading telecommunications provider in the UK. Our Broadband is received by a dedicated Internet connection and is tailored with filters to our specific needs. The procedures for ongoing management and review are:

- The school will work with Schools Broadband and 123 ICT to ensure that systems are reviewed and any improvements are implemented.
- If staff or pupils discover unsuitable sites, the URL must be reported to a member of the 123ICT team who will then ensure that the URL is blocked.
- Any material that the school believes to be illegal must be reported to appropriate agencies (IWF or CEOP)

Managing E-mail and Communications:

E-mail is an essential means of communication for both staff and pupils. Directed e-mail use can bring significant educational benefits.

Staff: All staff are given a secure school e-mail address upon joining the school. The creation of these accounts is the responsibility of the school's Business Manager. Should any staff need to contact parents directly then they should use their school e-mail, or if relevant, the school mobile, otherwise all communications should be passed on by the school office. All personal contact details for staff members will remain private.

Pupils: In certain circumstances pupils may be given access to an approved Office 365 email account. This is likely to be in the context of a class email address rather than an individual email account.

In order to enable responsible and safe e-mail use, the following measures are in place:

- Pupils may only use approved Office 365 e-mail accounts.
- Pupils only have access to internal e-mail to teachers and fellow pupils.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Use of words included in the filtering/checking 'banned' list will be detected and logged.
- Pupils are taught how to use e-mail during Computing skills lessons from Year 1 upwards and educated in the risks and how best to manage them.
- Access in school to external personal e-mail accounts may be blocked by the School's Broadband filtering systems.
- The school reserves the right to monitor user's e-mail accounts provided by the school.

- Outside school pupils are advised not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.

Password Protection:

Upon joining the school, the system administrator creates a unique username and generic password for each child that they can use to log into the school's network. The children's passwords can be reset and changed by the system administrator using a networked device.

In Key Stage 1, the children do not change their default password and the class teacher keeps a record of their log-in details. In Key Stage 2, the children are asked to change their passwords, choosing one that they will be able to remember. Their class teacher will also keep a record of their changed log-in details. As part of computing lessons and E-safety teaching, children are taught about the importance of keeping their personal details, including passwords, private.

Managing Published Content and Images:

Our school website celebrates pupils' work, promotes the school, publishes resources and acts as a communication tool. Publication of information on the Woodstock CE Primary School website is carefully considered from a personal and school security viewpoint.

Contact details available on the website are school address, e-mail and telephone number. Staff or pupils' personal information must not be published and all images used will comply with the conditions below:

- Children's names are published as their first name only e.g. Trevor, or if required, first name and last name initial e.g. Graeme B.
- Adults may be referred to by their full name, but only with their agreement.
- Any images of children must **not** be labelled with their names.
- Children will only be shown in photos where they are suitably dressed.
- Completed consent forms from parents or carers must be obtained before images of pupils are electronically published. A master list is available and updated by the school office staff.
- While images may be taken by parents, it is requested that they are not shared in the public domain.
- All digital images are securely stored and disposed of in accordance with the Data Protection Act.

Managing Information Services:

Woodstock CE Primary School commit to take due care in regard to managing the provision of Information Services to support secure and appropriate access. The measures outlined in this Policy include:

- Network servers are kept securely in a locked room.
- The security of the school information system is reviewed regularly 123 ICT and Talk Straight Ltd.
- The school keeps the network secure with a number of group policy settings and permissions which only allow certain users to use portable storage devices and to access and open certain drives and files.
- The school reserves the right to monitor user areas and equipment provided by the school.
- Sophos anti-virus software updates automatically every hour. Staff are also encouraged to install Sophos at home to increase security.
- The school uses Internet firewall and filters provided by Talk Straight Ltd.
- For fire safety network server backups of user data are taken daily and stored remotely using online servers.

d. Social Networking and Personal Publishing

Parents and teachers need to be aware that the Internet has emerging online spaces and social networks which allow individuals to publish unmediated content. Social networking sites can connect people with similar or even quite different interests. Guests can be invited to view personal spaces and leave comments, over which there may be limited control. There is increasing educational potential of such tools, for example in the use of blogs and wikis to improve writing.

However, whilst direct access to social networking sites in school is limited and regulated, a significant number of pupils in upper KS2 now use social networking out of school hours on a regular basis. As a school, we recognise that they may need guidance and support in knowing how to stay safe in such sites, and parents may not know what advice to give them. Pupils need to be encouraged to consider the implications of uploading personal information and the relative ease of adding the information and the practical impossibility of removing it.

Pupils need to be taught the reasons for caution in publishing personal information and photographs on the Internet and in particular on social networking sites. Our E-safety Policy aims to provide guidance and council on keeping safe within social networking and personal publishing. Specific council is:

- Within school hours, the school blocks access to social networking sites unless a specific use is approved.
- Pupils are advised never to give out personal details of any kind, which may identify them and / or their location. Examples would include real name, address, mobile or landline phone numbers, school attended,
- Pupils are advised not to place personal photos on any social network space. They should consider how public the information is and consider using private areas.
- Staff must ensure their profiles on social networking sites are private and not to add past or present pupils as friends.
- Staff should not give out their personal email address to parents. All communications must go through the school office.
- Staff and pupils are advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Pupils are encouraged to invite known friends only and deny access to others. They are advised not to publish specific and detailed private thoughts.

We very much acknowledge that we cannot act in isolation and parent's co-operation in supporting these steps is greatly appreciated.

e. E-Safety Complaints

For safe practice to be a reality, pupils, teachers and parents must know how to submit a complaint. The Complaints Policy is available on the school website and in paper form from the school office. If parents, pupils or members of the public have concerns they should:

1. Discuss their concerns with the member of staff most directly involved and, if not satisfied;
2. Discuss their concerns with a senior member of staff and, if not satisfied;
3. Discuss their concerns with the Headteacher. If the Headteacher considers she can do no more to resolve the complaint it will be stated explicitly that the complainant can write to the Chair of Governors if not satisfied.

Complainants are encouraged to state what actions they feel might resolve the problem at any stage.

Prompt action will be taken if a complaint is made. A minor transgression of the rules may be dealt with by the teacher. Other situations could potentially be serious and a range of sanctions will be required, linked to the school's Disciplinary Policy.

Formal complaints of Internet misuse will be dealt with by a member of the Leadership Team. Any complaint about staff misuse must be referred to the Headteacher.

Complaints of a child protection nature will be dealt with in accordance with school child protection procedures.

Only where all these avenues have been tried and found unsatisfactory should the complainant take a complaint to the Chair of Governors or Clerk to the Governing Body.

f. Risk Assessments

In-line with commitments made within this Policy, the school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never appear on a school computer. All Internet access at Woodstock CE Primary School is filtered through the LA filtering system. Whilst very robust in their practises around Internet use, neither the school, 123 ICT nor Schools Broadband can accept liability for the material accessed, or any consequences resulting from Internet use.

In order to ensure that risk is minimised, the following actions are taken:

- Methods to identify, assess and minimise risks are reviewed regularly.
- Staff, parents, governors and advisers work to establish agreement that every reasonable measure is being taken.
- Pupils are taught to consider the risks of using the Internet and how best to manage them.
- The Headteacher will ensure that the E-safety Policy is implemented and compliance with the Policy monitored.

6. Guidelines by Technology

The Policy is applied across a range of technologies that continue to expand and evolve. In addition to computers and tablet devises commonly used to access the Internet or enable communications, this Policy outlines clear guidelines as they apply to other known and used technologies. Specifically:

a. Video Conferencing

Video conferencing, including Skype and FaceTime, enables users to see and hear each other between different locations. It is a 'real time' interactive technology and has many uses in education. The practices below aim to ensure that we apply our e-safety commitments to video conferencing.

Equipment:

- All video conferencing equipment in the classroom must be switched off when not in use and not set to auto answer.
- IP video conferencing must use the educational broadband network to ensure quality of service and security rather than the Internet.
- Video conferencing contact information will not be put on the school website
- The equipment must be secure and locked away when not in use.

Users:

- Video conferencing will be supervised by an appropriate adult at all times.
- Pupils must ask permission from the teacher before making or answering a videoconference call.

Content:

- When a lesson is to be recorded, written permission will be given by all sites and participants. The reason for the recording must be given and the recording of video conference must be clear to all parties at the start of the conference.
- The school will establish dialogue with other conference participants before taking part in a videoconference. If it is a non-school site, checks will be made to ensure that they are delivering material that is appropriate for the audience.

b. Internet enabled mobile phones and handheld devices

Increasingly, a greater number of young people have access to new and sophisticated Internet-enabled devices such as SMART mobile phones, tablets and music players. It is important that whilst the school recognises the potential advantages these devices can offer, there are clear and enforceable rules for their use in school, particularly when they give access to the Internet, and allow pictures and information to be remotely posted to a website or weblog.

Our policy is that pupils are not allowed to have personal mobile phones or other similar devices in school. Parents may request that such devices are kept at the School Office for pupils who may need them on their journey to and from school.

However, in acknowledgement of the growing use, pupils will be taught about the benefits and risks, the legal and moral implications of posting photos and personal information from mobile phones to public websites, and how the data protection and privacy laws apply.

c. Online Gaming

Online gaming can be a helpful and engaging way of developing learning through play with a range of educational content presented through games to support literacy, maths, problem solving, strategy or coding. Controlled use may be supported within the classroom but always through screened individual log-in programs or via teacher lead activity where fit for use and appropriate access settings have been pre-assessed.

However, we also recognise from our recent Internet Survey that gaming plays a key part in recreational play in the home setting or when with friends. We have therefore outlined some best practice guidance from Microsoft which will help to support and keep children safe when gaming online.

Making safe choices:

All games all have age guidance ratings so that content can be assessed as appropriate. Check the ratings of the games your children want to play. In the UK most games for consoles or online have a PEGI rating which can be found on pack or searched for via the PEGI website. You can use these ratings as you discuss the most appropriate games with your child. In line with our safeguarding policy we would look to protect children from content that is violent or inappropriate by advising strongly that children are not permitted access to games with a PEGI rating greater than 7.

Beyond the content rating, selecting games that are well-known or those from reputable sites will reduce the risk of downloading viruses or sharing data in an unprotected way. You can also review the game's terms of play to find out how the game service monitors players and responds to abuse and read the site's privacy policy to learn how it will use and protect children's information.

Being aware of the risks:

Games that have no on-line connection, no entry of personal data or passwords and that are user only controlled do not pose a potential e-safety risk, however, to add an extra dimension to a game there is increasingly a multiplayer element, where players often communicate via integrated chat or verbally with microphone or a headset.
Many games – from simple chess to first-person adventure games, where thousands of players participate at the same time – include these features. The presence of such a large online community of anonymous strangers and the unfiltered, unmoderated discussions, can pose a variety of potential risks such as:

- Inadvertently giving away personal information, including password, email or home address or age.
- Inappropriate contact or behaviour from other gamers
- Buying or selling virtual, in-game property – for example high-level characters – where there is real money involved.
- Disposing of game consoles, PCs and mobile devices without deleting your personal information and account details.
- Playing games for many hours at a time with the danger of becoming addicted.

Recommended solutions:

Gaming can be an enriching learning experience with some simple steps to keep safe:

- Play online games only when you have effective and updated antivirus software and firewall running.
- Play only with authorised versions of games which you have purchased from the correct sources and for which you have a licence. Verify the authenticity and security of downloaded files and new software by buying from reputable sources.
- Choose a user name and password with your child that does not reveal personal information. Similarly, if the game includes the ability to create a personal profile, or where contact can be made by other players make sure that no personal information is given away.
- Read the manufacturer or hosting company's terms and conditions to make sure there will not be any immediate or future hidden charges.
- When disposing of your gaming device either by selling, scrapping, giving away or donating, ensure all of your personal information and your account details have been deleted.
- Set guidelines and ground rules for your children when playing online. This could include time limitations, parent entered passwords or game play only in communal areas

d. Emerging Technologies

Many emerging communications technologies offer the potential to develop new teaching and learning tools. A risk assessment needs to be undertaken on each new technology, and effective practice in classroom should be developed. The contents of this Policy are regularly reviewed and updated in light of the on-going changes to modern technologies.

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

7. Behaviours & Sanctions

A critical part of our E-safety Policy which applies across all technologies are the behaviours we seek to embed and the sanctions pupils or staff may face if their actions put their or others E-safety at risk.

Behaviours

Personal Information is Personal

Pupils learn to never give out personal details such as name, address, date of birth, school
User names and passwords should not contain personal information

Treat others online as you do in the real world

Pupils learn that online bullying and harassment are potential problems that can have a serious effect on children. They are aware that causing upset or harm online will follow the same sanctions as outlined in our

Strangers Online are still strangers

Pupils learn to recognise that friends are people we know and see regularly as part of our everyday lives. Online "friends" are strangers and invitations to meet them in the real world should be reported.

Evaluate what you see and do

Pupils learn to evaluate everything they read, and to refine their own publishing and communications with others via the Internet. They are supported in learning to evaluate internet content as outlined in the section

What to do if something isn't right

Pupils learn that if they know or feel something isn't right that they should speak to, or contact an adult immediately.

Sanctions:

The school would take immediate action if pupils or staff were to put themselves or others at risk. There may be occasions when the police must be contacted. Early contact will be made to establish the legal position and discuss strategies.

Pupils: Sanctions within the school Behaviour Policy will apply:

- Interview/counselling by a member of the Leadership Team
- Informing, and if appropriate, meeting with parents or carers
- Removal of Internet or computer access for a period.

Staff: As a school we have formally adopted Oxfordshire County Council's Discipline Procedures for all Employees in Schools. It is essential for staff to use the Internet, including social media in a responsible and professional manner both in school and out of school, in order to ensure the privacy and safety of all employees, pupils, parents and members of the wider school community.

Effective support, supervision and counselling of staff by a member of the Leadership Team should reduce the need to use the disciplinary procedure. Incidents relating to irresponsible Internet use will be brought to the employee's attention as soon as possible in an effort to resolve the situation informally, however if appropriate more formal procedures will be set in motion in-line with OCC guidance.
Any incidents will be reflected on by the E-safety Committee and retraining organised if appropriate.

8. Learning to Evaluate Internet Content

Developing best practice Internet use is imperative. Parents and teachers can help pupils learn how to distil the meaning from the mass of information provided on the Internet.

Often the quantity of information is overwhelming and staff guide pupils to appropriate websites, or teach search skills. Information received via the Internet, e-mail, or text message requires good information handling skills. Our approach is to offer younger pupils a few good sites as this is often more effective than an Internet search. Respect for copyright and intellectual property rights, and the correct use of published material are taught.

Above all pupils need to learn to evaluate everything they read and to refine their own publishing and communications with others via the Internet. Specifically:

- The school Internet access is designed expressly for pupil use and includes filtering appropriate to the age of pupils.
- Pupils are taught what Internet use is acceptable and what is not and are given clear objectives for Internet use.
- Internet access is planned to enrich and extend learning activities.
- Staff guide pupils in on-line activities that support the learning outcomes planned for the pupils' age and maturity.
- ICT skills lessons are used to educate pupils in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation. This is reinforced by teachers when using the internet within their classroom.
- The school ensures that copying and subsequent use of the Internet derived materials by staff and pupils complies with copyright law.
- Pupils are taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy

9. Appendices

a. Protecting Personal Data

Personal data will be recorded, processed, transferred and made available in compliance with the Data Protection Act 1998.

The Data Protection Act 1998 ('the Act') gives individuals the right to know what information is held about them and it provides a framework to ensure that personal information is handled properly. It promotes openness in the use of personal information.

Under the Act every organisation that processes personal information (personal data) must notify the Information Commissioner's Office, unless they are exempt. The Data Protection Act 1998 applies to anyone who handles or has access to information concerning individuals. Everyone in the workplace has a legal duty to protect the privacy of information relating to individuals. The Act sets standards (eight data protection principles), which must be satisfied when processing personal data (information that will identify a living individual).

The Act also gives rights to the people the information is about i.e. subject access rights lets individuals find out what information is held about them. The eight principles are that personal data must be; processed fairly and lawfully, processed for specified purposes, adequate, relevant and not excessive, accurate and up-to-date, held no longer than is necessary, processed in line with individuals' rights, kept secure and transferred only to other countries with suitable security measures.

b. Acceptable Internet Use Policy for Staff

The computer system is owned by the school, and may be used by pupils to further their education and by staff to enhance their professional activities including teaching, research, administration and management. The school's E-safety Policy has been drawn up to protect all parties – the pupils, the staff and the school. To ensure that staff are fully aware of their professional responsibilities when using information systems, they are asked to sign this code of conduct. Staff should consult the school's E-safety Policy for further information and clarification. Specifically:

- The information systems are school property and I understand that it is a criminal offence to use a computer for a purpose not permitted by its owner.
- I understand that school information systems may not be used for private purposes, without specific permission from the Headteacher.
- I understand that the school may monitor my network area and Internet use to ensure policy compliance.
- I will respect system security and I will not disclose any password or security information to anyone other than an appropriate system manager.
- I will not install any software or hardware without permission.
- I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will respect copyright and intellectual property rights.
- I will report incidents of concern regarding children's safety to the school's designated Child Protection Co-ordinator.
- I will ensure that any electronic communications with pupils are compatible with my professional role.
- I will promote E-safety with pupils in my care and will help them to develop a responsible attitude to system use and to the content they access or create.

The school may exercise its right to monitor the use of the school's information systems, including Internet access, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

I have read, understood and agree with Acceptable Use Policy.

Signed: Date:

c. E-Safety Contacts and References

Childnet International
http://www.childnet.com/resources

Childline
http://www.childline.org.uk

Think U Know (links to CEOP)
www.thinkuknow.co.uk

Child Exploitation and Online Protection Centre
www.ceop.gov.uk

Stop it now (child sexual abuse prevention campaign, for all adults)
www.stopitnow.org.uk

Parents Protect
www.parentsprotect.co.uk

E-Safety self-review tools provided by South West Grid for Learning
www.360safe.org.uk for schools and www.onlinecompass.org.uk for youth settings

Securus (Company supplying software to protect pupils from cyberbullying in schools)
www.securus-software.com

Internet Watch Foundation (IWF)
www.iwf.org.uk was set up by the UK internet industry to provide the UK internet 'Hotline' for the public to report potentially illegal online content.

CBBC Stay Safe
www.bbc.co.uk/cbbc/topics/stay-safe

Web Cam fact sheet
http://www.thinkuknow.co.uk/Documents/Webcam%20fact%20sheet%202.pdf

BBC Chat Guide
http://www.bbc.co.uk/chatguide/

Becta
http://www.becta.org.uk/schools/esafety

e-Safety in Schools
http://www.kenttrustweb.org.uk?esafety

Grid Club and the Cyber Cafe
http://www.gridclub.com

Internet Safety Zone
http://www.internetsafetyzone.com/ Kent Primary Advisory e-Safety Pages
http://www.kented.org.uk/ngfl/ict/safety.htm

Kidsmart
http://www.kidsmart.org.uk/ NCH – The Children's Charity
http://www.nch.org.uk/information/index.php?i=209 NSPCC
http://www.nspcc.org.uk/html/home/needadvice/needadvice.htm Schools e-Safety Blog
http://clusterweb.org.uk?esafetyblog

Schools ICT Security Policy
http://www.eiskent.co.uk (broadband link) Stop Text Bully
www.stoptextbully.com

Report it:

Thames Valley Police – for suspected criminal activity
http://www.thamesvalley.police.uk/reptcr/reptcr-repform.htm

Oxfordshire County Council website – for child safeguarding concern
http://www.oxfordshire.gov.uk/cms/public-site/child-social-care

CEOP – report a child in danger of abuse. Children can self-report.
http://www.ceop.police.uk/safety-centre/

Virtual Global Taskforce – Report Abuse
http://www.virtualglobaltaskforce.com/

Internet Watch Foundation – report child sexual abuse content http://www.iwf.org.uk/

Professionals Online Safety Helpline – 0844 3814772 helpline@saferinternet.org.uk

d. Children's Code of Conduct for Responsible use of Technology

The school has computers and tablet devices with access to the Internet to support our learning. These rules will help keep us safe and help us be fair to others.

Using the Computers:

- I will only access the computer system with the login and password I have been given.
- I will not access other people's files.
- I will not bring in memory sticks or CDs from outside school and try to use them on the school computers.

Using Mobile Technology:

- I will only use the iPads and other tablet devices when I have been given permission to by my teacher.
- I will use the tablet responsibly and make sure that it is returned to the trolley after I have used it.
- I will not use any Apps that I have not been given permission to use.
- I will not take photographs or film children or adults without their permission.

Using the Internet:

- I will ask permission from a teacher before using the Internet.
- I will report any unpleasant material to my teacher immediately because this will help protect other pupils and me.
- I understand that the school may check my computer files and may monitor the Internet sites I visit.
- I will not complete and send online forms without permission from my teacher.
- I will not give my full name, my home address or telephone number when using the Internet.

Using E-mail:

- I will ask permission from a teacher before sending an e-mail.
- I will immediately report any unpleasant messages sent to me because this will help protect other pupils and me.
- I understand that e-mail messages I receive or send may be read by others.
- The messages I send will be polite and responsible.
- I will only e-mail people I know, or my teacher has approved.
- I will only send an e-mail when it has been checked by a teacher.
- I will not give my full name, my home address or telephone number.
- I will not use e-mail to arrange to meet someone outside school hours.

e. ANTI-CYBERBULLYING POLICY

We aim to ensure that children are safe and feel safe from bullying, harassment and discrimination under the Stay Safe Every Child Matters Agenda. Our school is committed to teaching children the knowledge and skills to be able to use ICT effectively, safely and responsibly.

Cyber bullying Defined:

Cyber bullying can be defined as the use of Information and Communications Technology (ICT), particularly mobile phones and the internet, deliberately to upset someone else. It can be an extension of face-to-face bullying, with technology providing the bully with another route to harass their target. However, it differs in several significant ways from other kinds of bullying: the invasion of home and personal space; the difficulty in controlling electronically circulated messages; the size of the audience; perceived anonymity; and even the profile of the person doing the bullying and their target.

Aims of Policy:

- To ensure that pupils, staff and parents understand what cyber bullying is and how it can be combated.
- To ensure that practices and procedures are agreed to prevent incidents of cyber bullying.
- To ensure that reported incidents of cyber bullying are dealt with effectively and quickly.

Understanding Cyber bullying:

- Cyber bullying is the use of ICT (usually a mobile phone and or the Internet) to abuse another person.
- It can take place anywhere and involve many people.
- Anybody can be targeted including pupils and school staff.
- It can include threats, intimidation, harassment, cyber-stalking, vilification, defamation, exclusion, peer rejection, impersonation, unauthorised publication of private information or images etc.

Procedures to Prevent Cyber bullying:

- Staff, pupils, parents and governors to be made aware of issues surrounding cyber bullying.
- Pupils and parents will be urged to report all incidents of cyber bullying to the school.
- Staff CPD will assist in learning about current technologies.
- Pupils will be involved in developing and communicating this policy.
- Pupils will learn about cyber bullying through PSHE, assemblies, Anti-bullying Week activities and other curriculum projects.
- Pupils will sign an Acceptable Use of ICT Contract.
- Parents will be provided with information and advice on how to combat cyber bullying
- Parents will be expected to sign an Acceptable Use of ICT contract and to discuss its meaning with their children.
- Pupils, parents and staff will be involved in reviewing and revising this policy and school procedure.
- All reports of cyber bullying will be investigated, recorded, stored in the Headteacher's office and monitored regularly.
- The Local Authority can provide support and assistance in dealing with incidents of cyber bullying and can be contacted by staff and parents. The police will be contacted in cases of actual or suspected illegal content.

f. Internet Safety Check

It is good practice to discuss these points with pupils at the start of the school year, the start of a project requiring Internet use, or if revision of Acceptable Internet Use is necessary.

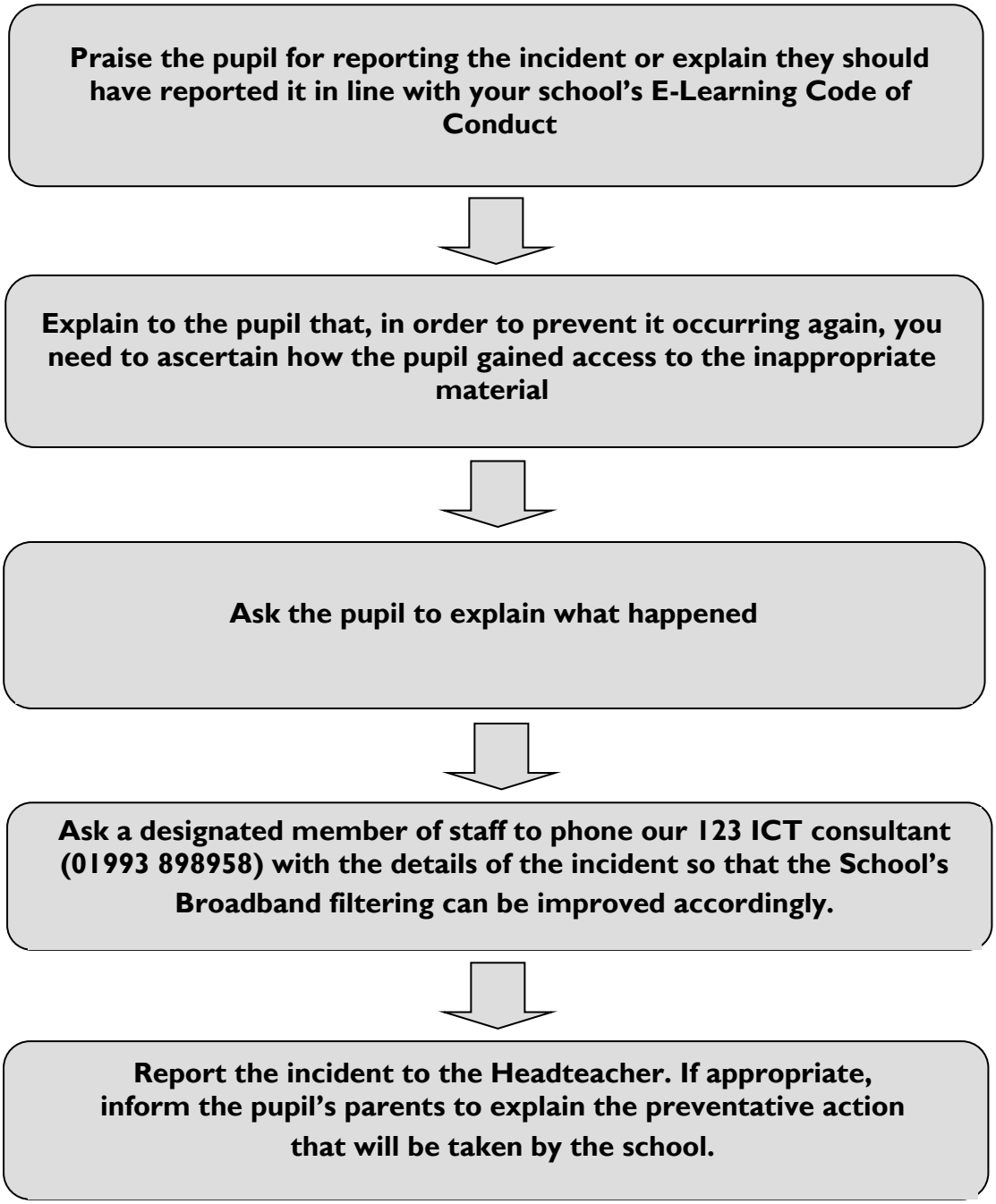
- **Only use the Internet when there is a teacher or other adult present to supervise or when you have been given specific permission.**
- **Only use your own login name and password. Never use another person's details.**
- **Never give out your address, phone number or arrange to meet someone over the Internet.**
- **All e-mails, messages in forums and text messages should be polite, appropriate and sensible. Do not send any e-mail or text message which could cause upset.**
- **If you receive a rude or offensive message you must report it to a teacher immediately. Do not pass on rude or offensive messages. What may seem funny to you may not be funny to someone else.**
- **If you see anything offensive or if you feel uncomfortable about anything, report it to your teacher or to an appropriate member of staff.**
- **Be aware that the school may check your computer files and monitor the Internet sites you visit.**
- **Ask an adult if you are unsure that a web source is reliable and information you are going to use is accurate.**
- **You and your parents should have signed the school Internet Agreement. You will be breaking that Agreement if you deliberately break these rules. This could result in you losing your Internet access at school.**

Draw pupil's attention to the poster on the wall in the classroom regarding sensible conduct whilst using the Internet. They can refer to this anytime they need a reminder.

g. Guidelines on Inappropriate Internet Access

Whilst using the Internet during school hours, a pupil **accidentally** finds a website displaying inappropriate material. What should you do?

Use this step-by-step guide to help you follow the correct procedure for reporting inappropriate materials from the Internet.



h. Copyright Release & Digital Video Information

Woodstock CE Primary School

Copyright Release

The school may produce printed publications and/or a school web site which may include examples of pupil's work and/or photographs of pupils. No child's work will ever be used without his/her permission and we take the issue of child safety very seriously which includes the use of images of pupils. Including images of pupils in school publications and on the school website can be highly motivating for the pupils involved, and provides a good opportunity to promote the work of the school. However, schools have a duty of care towards pupils, which means that pupils must remain unidentifiable, reducing the risk of inappropriate contact, if images are used in this way.

We ask that parents' consent to the school publishing their children's work and to the taking and using of photographs and images of their children subject to strict confidentiality of personal information. (This can be changed at any time by request to the Headteacher or ICT Co-ordinator).

Digital Video

Digital video is an exciting medium which can motivate and inspire pupils. Research has shown that using digital video in education can help encourage creativity, motivate and enthuse pupils, and improve communication and team-working skills.

At **Woodstock CE Primary School** we intend to use digital video as part of our learning and teaching, and for the recording of school productions and events.

We ask that parents give written consent to their child taking part in the production of digital video, and/or appearing in films.

Whereas the risks of using digital video in education are minimal, schools have a duty of care towards pupils. This means that pupils will remain unidentifiable, reducing the risk of inappropriate contact, if images or examples of their work (including digital video) are used on the school website. All digital video work at Woodstock CE Primary School is underpinned by our Acceptable Use and Internet Safety Policies.

Woodstock CE Primary School
Shipton Road, Woodstock OX20 1LL

Telephone
01993 812209

Email
office.3145@woodstock.oxon.sch.uk

Website
www.woodstock.oxon.sch.uk

Headteacher
Lisa Rowe

Permission and Copyright Release

I consent to photographs and digital images of the child named above, appearing in printed publications or on the school website. I understand that the images will be used only for educational purposes and that the identity of my child will be protected. I also acknowledge that the images may also be used in and distributed by other media, such as CD-ROM, as part of the promotional activities of the school.

I further consent to examples of my child's work being published on the school web site or in other media, subject to strict confidentiality of personal information as compliant with the Data Protection Act.

Parent/Carer Signature Date

Digital Video

I consent to my child taking part in **Woodstock CE Primary School** projects using digital video. I consent to my child taking part in the production of digital videos and appearing in films. I understand that films may be made available on the school website or used in other school promotional activities.

Parent/Carer Signature Date

i. E-SAFETY CODE OF CONDUCT

E-Safety Code of Conduct

Dear Parent/Carer,

As part of our curriculum we encourage pupils to make use of educational resources available on the Internet. Access to the Internet enables pupils to conduct research and obtain high quality educational resources from libraries, museums, galleries and other information sources from around the world.

To guard against accidental access to materials which are inappropriate in school our access to the Internet is provided by Schools Broadband, a specialist division of Talk Straight Ltd. However, it is not possible to provide a 100% assurance that pupils might not accidentally come across material which would be inappropriate.

Therefore, before they access the Internet we would like all pupils to discuss the E-Learning Code of Conduct with their parents/carers and then return the signed form to your child's class teacher.

We believe that the educational benefits to pupils from access to the Internet, in the form of information resources and opportunities for collaboration, far outweigh the potential disadvantages.

During lesson time teachers will guide pupils toward specific materials and educational resources. Where pupils are given permission to access the Internet outside lessons they must agree to access only those sites that are appropriate for use in school and use the e-learning resources appropriately.

Yours sincerely

****

Pupil: Date: Year Group:

My parents and I have read the E-Learning Code of Conduct and I agree to follow it.

Pupil Signature Date

Parent:

As parent or carer, I have read, discussed and explained the E-Learning Code of Conduct to my son/daughter. I understand that if he/she fails to follow this code, his/her individual access may be withdrawn and I will be informed.

Parent/Carer Signature Date

j. E-Safety Incident Recording Form

Please record sufficient detail to enable the monitoring of incidents.

Type of Incident:	✓	**System Location:**	✓
Bullying (cyber bullying)		Library	
Grooming		Classroom	
Sharing inappropriate messages		Corridor	
Sending inappropriate images		Outside school premises	
Hacking or virus spreading		Other (record in **description** below)	
Accessing racist, sexual or homophobic material			
Sharing racist, sexual or homophobic material		**Device accessed on:**	✓
Accessing religious hate material		Laptop	
Sharing religious hate material		Desktop computer	
Accessing pornographic material		iPad/Tablet	
Sharing pornographic material		Mobile phone	
Other (record in **description** below)		Other (record in **description** below)	

Date:	**Time:**
Description of what happened:	

Accidental Access:	**Deliberate Access:**

Child/ren Involved:	Year	SEN	Disability	Ethnic Group	Involvement in Incident

Member of staff recording the incident:
Role:

Other staff involved:
Role:

Action Taken:		
If appropriate:	Yes ✓	No ✓
Have you copied Incident Form for class teacher?		
Have you had contact with the parents/carers of all children involved? If Yes, by phone / letter? Date of contact:		
Are any other agencies involved? If Yes, which agencies? If Yes, and the incident was prejudice-motivated, consult Local Authority as to whether a Hate Crime report is appropriate.		
Does the incident require Police/CEOP involvement?		

Signed:

Name:

Date:

Status:	✓
Resolved	
Unresolved	
Further intervention needed	
123 ICT informed (if appropriate)	

File THREE Copies (tick when actioned)	**Headteacher**	**Child's File**	**E-safety File**
Details of any subsequent actions or follow-up: (Include dates)			