Driffield Junior School

E-Safety Policy

Development / Monitoring / Review of this Policy

This e-safety policy has been developed by a working group made up of:

- Headteacher (Linda Laird)
- E-Safety Officer Coordinator (Rachel Westerby)
- Designated Safeguard Lead (Lynne Kneeshaw)
- School Business Manager (Karen Hamilton)
- Child Protection Governor (Liz Sutcliff)

Schedule for Development / Monitoring / Review

This e-safety policy was approved by the *Governing Body:*	
The implementation of this e-safety policy will be monitored by the:	Headteacher (Linda Laird), E-safety Coordinator (Rachel Westerby), Designated Safeguard Lead (Lynne Kneeshaw), School Business Manager (Karen Hamilton) and School Governors.
Monitoring will take place at regular intervals:	Twice annually
The *Governing Body Committee* will receive a report on the implementation of the e-safety policy generated by the monitoring group (which will include anonymous details of e-safety incidents) at regular intervals:	Annually
The E-Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place. The next anticipated review date will be:	November 2017
Should serious e-safety incidents take place, the following external persons / agencies should be informed:	EHASH

Schedule for Development / Monitoring / Review

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Random sample monitoring of internet activity
- Sample surveys / questionnaires/discussions with
    - pupils
    - parents / carers
    - staff

Scope of the Policy

This policy applies to all members of the *school* (including staff, pupils, volunteers, parents / carers, visitors) who have access to and are users of school ICT systems, both in and out of the *school*.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the *school* site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school

The Driffield Junior School will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school.

Roles and Responsibilities

The following section outlines the e-safety roles and responsibilities of individuals and groups within the *school*:

Governors:

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about e-safety incidents and monitoring reports. A member of the Governing Body has taken on the role of Safeguarding Governor which is a combined role which includes *E-Safety.*

The role of the Safeguarding *Governor* will include:

- meetings with the Designated Safeguard Lead
- monitoring of e-safety incident logs
- monitoring of filtering / change control logs
- reporting to relevant Governors meeting

Headteacher and Senior Leaders:

- The Headteacher has a duty of care for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to the E-Safety Co-ordinator.
- The Headteacher and deputy Headteacher have procedures in place to be followed in the event of a serious e-safety allegation being made against a member of staff
- The Headteacher is responsible for ensuring that the E-Safety Coordinator , Designated Safeguarding Lead and other relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.
- The Senior Leadership Team will receive reports from the E-Safety Co-ordinator when required.

E-Safety Coordinator:

- leads the e-safety working group
- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- provides training and advice for staff
- liaises with technical staff
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments,
- work collaboratively with the Designated Safeguard Lead to record e-safety incidents and to review incident logs. The Designated Safeguard Lead will meet with the Safeguarding Governor to discuss current issues.
- attends relevant meeting such as Governors meeting committee

- reports to Senior Leadership Team

School Business Manager:

The school business manager is responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets required e-safety technical requirements and Local Authority E-Safety Policy / Guidance.
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- the filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person. The East Riding Local Authority currently manages the schools filtering.
- that they keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant.
- that the use of the network / internet / remote access / email is monitored in order that any misuse / attempted misuse can be reported to the Headteacher for investigation / action / sanction

Teaching and Support Staff

Teaching and Support Staff are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP)
- they report any suspected misuse or problem to the Headteacher/ E-Safety Coordinator / Designated Safeguarding Lead/School Business Manager for investigation / action / sanction
- all digital communications with pupils / parents / carers should be on a professional level and only carried out using official school systems
- e-safety issues are embedded in all aspects of the curriculum and other activities
- pupils understand and follow the e-safety and acceptable use policies
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, i-pads, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- in lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Designated Safeguarding Lead

The Designated Safeguarding Lead is trained in e-safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying

E-Safety Working Group

The E-Safety Working Group provides a consultative, with responsibility for issues regarding e-safety and of the monitoring

the e-safety policy including the impact of initiatives. The group will also be responsible, via the E-safety coordinator to report to the Governing Body.

Members of the E-safety Working Group will assist the E-Safety Coordinator with:

- the production / review / monitoring of the school e-safety policy / documents.
- mapping and reviewing the e-safety curricular provision – ensuring relevance, breadth and progression
- monitoring network / internet / incident logs
- consulting stakeholders – including parents / carers and the pupils about the e-safety provision
- monitoring improvement actions identified through use of the E-safety self-review tool

Pupils

Pupils:

- are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Policy
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand policies on the use of mobile devices, digital cameras and i-pads. They should also know and understand policies on the taking / use of images and on cyber-bullying.
- should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy and Acceptable Use agreement covers their actions out of school.

Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about national / local e-safety campaigns / literature. Parents/ carers will be encouraged to support Driffield Junior in promoting good e-safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- their children's personal devices in the school.

Policy Statements

Education –pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in e-safety is therefore an essential part of the school's e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience.

E-safety is a focus in all areas of the curriculum and staff should reinforce e-safety messages across the curriculum. The e-safety curriculum will be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned e-safety curriculum should be provided as part of assemblies, computing lessons as well as a part of the cross-curricular lessons. E-safety learning should be regularly revisited
- Key e-safety messages will be reinforced as part of a planned programme of assemblies
- **P**upils will be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.

- Pupils will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils will be helped to understand the need for the pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school
- Staff will act as good role models in their use of digital technologies the internet and mobile devices
- In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.

Education – parents / carers

There are potentially some parents and carers that have a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line behaviours. Parents may sometimes underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters, newsletters, web site
- Parents / Carers afternoon and evenings sessions
- High profile events / campaigns eg Safer Internet Day
- Reference to the relevant web sites / publications

Education & Training – Staff / Volunteers

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal child protection/ e-safety training will be made available to staff. This will be regularly updated and reinforced.
- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Agreements.
- This E-Safety policy and its updates will be presented to and discussed by staff in staff meetings.
- The E-Safety Coordinator/ Designated Safeguarding Lead will provide advice / guidance / training to individuals as required.

Training – Governors

Governors will take part in e-safety training / awareness sessions, with particular importance for those who are members who are Safeguarding governors:

- Attendance at training provided by the Local Authority or other relevant organisation.
- Participation in school training / information sessions for staff or parents (this may include attendance at assemblies / lessons).

Technical – infrastructure / equipment, filtering and monitoring

Driffield Junior school computing system is managed by an outside provider and the local authority. Driffield Junior School is responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented.

- School technical systems is be managed in ways that ensure that the school meets recommended technical requirements
- There are reviews of the safety and security of school technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted

- All users will have clearly defined access rights to school technical systems and devices.
- All users in years 5 and 6 will be provided with a username and secure password by Rachel Westerby who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password.
- Karen Hamilton along with Primary tech is responsible for ensuring that software licence logs are accurate and up to date.
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the East Riding of Yorkshire Council by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored.
- The school has provided enhanced / differentiated user-level filtering
- School technical staff sample monitor activity of users and users are made aware of this in the Acceptable Use Agreement.
- An appropriate system is in place (via record of concern) for users to report any actual / potential technical incident / security breach to either Rachel Westerby or Karen Hamilton.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. The school infrastructure and individual workstations are protected by up to date virus software.
- An agreed login is in place for the provision of temporary access of "guests" (eg trainee teachers, supply teachers, visitors) onto the school systems.
- Driffield Junior School follows the E-riding acceptable use policy regarding the extent of personal use that users (staff / students / pupils / community users) and their family members are allowed on school devices that may be used out of school
- The acceptable use policy is followed regarding the use of removable media (eg memory sticks / CDs / DVDs) by users on school devices. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured

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

- Written permission from parents or carers is obtained from parents/ careers of children on the application form at the start of year 3 and only when this permission in received will photographs of pupils published on the school website.

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 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".
- Driffield Junior school has a Data Protection Policy.
- Driffield Junior school is registered as a Data Controller for the purposes of the Data Protection Act (DPA)
- Driffield Junior School has a 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 Data Protection clauses in all contracts where personal data may be passed to third parties.

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.

In line with the Acceptable use policy, 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 be password protected
- the device must offer approved virus and malware checking software

Communications

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

	Pupils				Staff and other adults			
Children Communications Technologies	Not Allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not Allowed	Allowed	Allowed at certain times	Allowed with staff permission
Mobile phones may be brought to school and handed in at the school office.		X						
Mobile phones may be brought to school						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	

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

- Pupils will be taught about e-safety issues, such as the risks attached to the sharing of personal details. They will 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 website and only official email addresses should be used to identify members of staff.

Social Media - Protecting Professional Identity

All schools and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools 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 Driffield Junior 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

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 Driffield Junior School or East Riding local authority.
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Unsuitable / inappropriate 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		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	

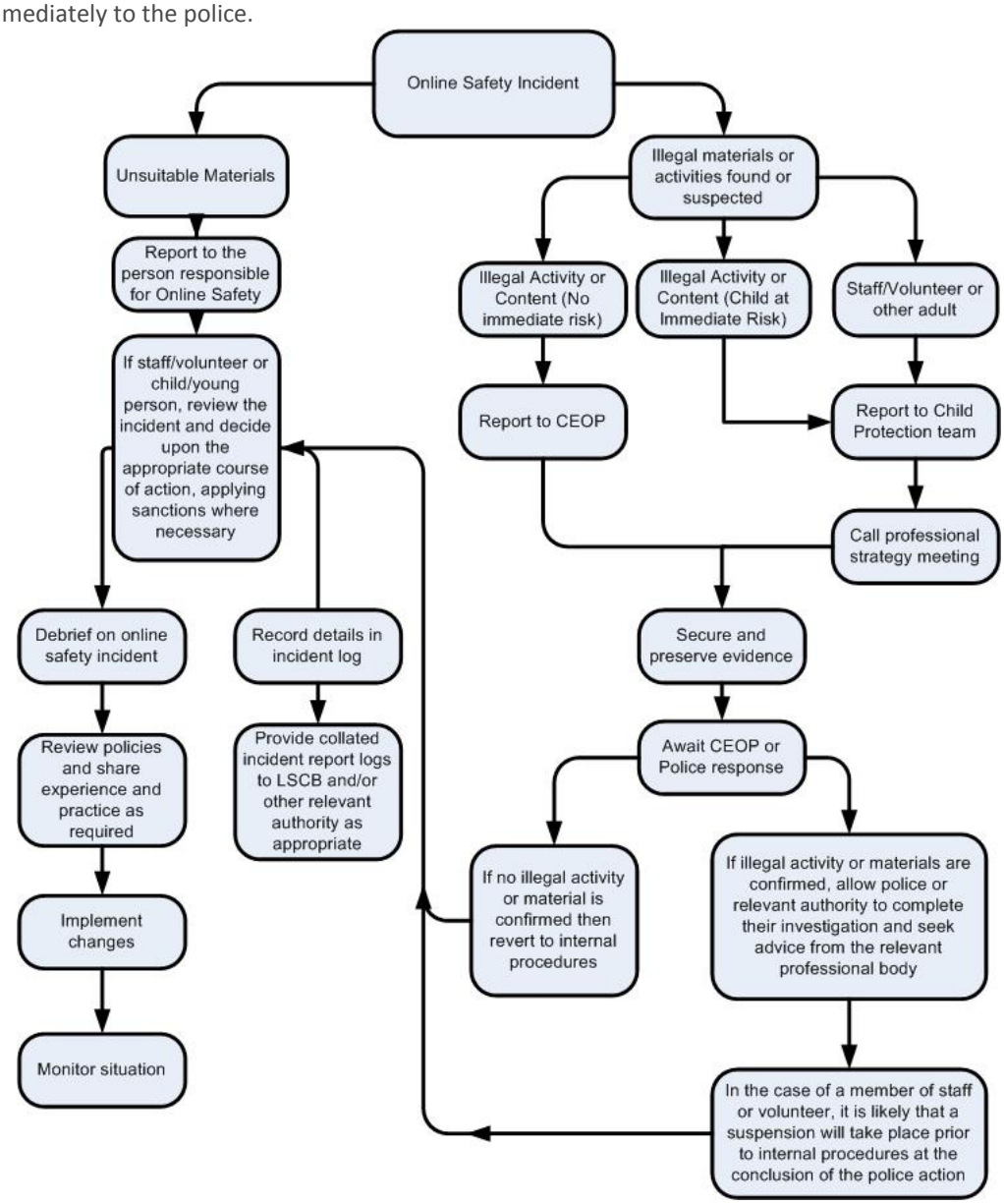
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)	X	
Creating or propagating computer viruses or other harmful files	X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)	X	

Responding to incidents of misuse

This guidance alongside the school disciplinary policy is for use if 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)

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 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 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.

School Actions & Sanctions

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. Incidents of misuse will be dealt with through the behaviour policy.