

Eaves Primary School

'Excellence in Everything'



E-Safety & Internet Policy

September 2023

Status	Statutory
Responsible Governors' Committee	Governing Body
Date first approved by GB	January 2016
Responsible Person	Mrs N Kearney
Review Date	September 2025
Last Amended Date	September 2023

Development / Monitoring / Review of this Policy

This e-safety policy has been developed by the E-Safety Group made up of:

- Headteacher – N Kearney
- Safeguarding Manager – J Lloyd
- Teachers – All Staff
- Governors – All Governors

Schedule for Development / Monitoring / Review

This e-safety policy was approved by the Governing Body on:	Autumn Term 2023
The implementation of this e-safety policy will be monitored by the:	Senior Leadership Team, Computing Subject Leader and ICT Technician
Monitoring will take place at regular intervals:	Bi-annually
The Governing Body 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 every 2 years 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:	Autumn Term 2025
Should serious e-safety incidents take place, the following external persons / agencies should be informed:	St Helens Council IT team, LA Safeguarding Officer, Police

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Local Authority procedures/filtering
- Monitoring logs of internet activity (including sites visited)
- Internal monitoring data for network activity

Scope of the Policy

This policy applies to all members of the school community (including staff, pupils, volunteers, parents/carers, visitors, community users) 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 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

The 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.

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 Officer/Computing Subject Leader.
- The Headteacher and another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff. (see flow chart on dealing with e-safety incidents – “Responding to incidents of misuse”).
- The Headteacher / Senior Leaders are responsible for ensuring that the E-Safety Officer and other relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.

E-Safety Officer and Computing Subject Leader: Miss K Heslin

- takes day to day responsibility for e-safety issues and have 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 school technical staff
- reports regularly to Senior Leadership Team

Technical staff:

Technical Staff and the Head Teacher are 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 any Local Authority guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- 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/Virtual Learning Environment/remote access/email is regularly monitored in order that any misuse/attempted misuse can be reported to the Headteacher and/or Governors for investigation/action/sanction

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 Agreement (AUA)
- they report any suspected misuse or problem to the Headteacher/Senior Leader/E-Safety Officer for investigation/action/sanction
- all digital communications with pupils/parents/carers should be on a professional level

- e-safety issues are embedded in all aspects of the curriculum and other activities
- pupils understand and follow the e-safety and acceptable use agreements
- 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

Safeguarding Manager:

The Safeguarding Manager should be 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

Pupils:

- 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, I pads and digital cameras. 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 covers their actions out of school, if related to their membership of the 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 and carers will be encouraged to support the school in promoting good e-safety practice and to follow guidelines on the appropriate use of digital and video images taken at school events

Policy Statements

As advised in "Teaching Online Safety in School," (DFE, June 2019) we adopt a whole school approach to the teaching of online safety that goes beyond teaching to include all aspects of school life, including culture, ethos, environment and partnerships with families and the community.

Education – pupils

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

- Planned e-safety sessions should be provided as part of Computing / PHSE / other lessons and should be regularly revisited
- Key e-safety messages should be reinforced through assemblies and pastoral activities
- Pupils should 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 should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet

- 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.
- It is accepted that from time to time, for good educational reasons, pupils may need to research topics (e.g. racism, drugs, discrimination) that would normally result in searches being blocked. In such a situation, staff can request that the Technical Staff temporarily remove those sites from the filtered list for the period of study. Any requests should have clear reasons for the need.

Education – parents / carers

Many parents and carers have only 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 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:

- Letters, newsletters, website, social media
- Parents / Carers evenings
- High profile events / campaigns eg Safer Internet Day
- Reference to relevant web sites / publications e.g.

www.swgf.org.ukwww.safeinternet.org.uk<http://www.childnet.com/parents-and-carers>

www.thinkyouknow.co.uk(CEOP)

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 e-safety training will be made available to staff including ThinkUKnow online training. This will be regularly updated and reinforced. An audit of the e-safety training needs of all staff will be carried out regularly.
- 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 / team meetings / INSET days.
- The Online safety Subject Leader will provide advice/guidance/training to individuals as required.

Technical – infrastructure / equipment, filtering and monitoring

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements
- There will be regular reviews and audits 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.
- The ICT Technician is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
- Internet access is filtered for all users by the Local Authority.
- The school has provided enhanced / differentiated user-level filtering
- School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.

- An agreed policy is in place for the provision of temporary access of “guests” (eg trainee teachers, supply teachers, visitors) onto the school systems.
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise. Staff must use One Drive to take personal data off the school site.

Clarification on Filtering and Monitoring will be delivered to all staff during the annual safeguarding training as recommended by the KCSIE guidance 2023. This is to raise awareness of the existing expectation.

Use of digital and video images

- The development of digital images 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, parent/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.
- 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 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 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, blog or social networking site particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website. Parents/carers provide this information by global consent.

Data Protection

GDPR provides 8 main rights for individuals and strengthens those that already exist under the current Data Protection Act 1998.

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights related to automated decision making and profiling

Personal data will be recorded, processed, transferred and made available according to GDPR 2018 which states that personal data must be:

- Accessed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary
- Accurate and kept up to date
- 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 purpose 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 appoints a Data Protection Officer
- It is registered as a Data Controller for the purposes of GDPR
- 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.
- A data protection impact assessment (DPIA) will:
 - be used to identify the most effective method of complying with the school's data protection obligations and meeting individuals' expectations of privacy
 - allow the school to identify and resolve problems at an early stage, thus reducing associated costs and preventing damage from being caused to the school's reputation which might otherwise occur
 - be carried out when using new technologies or when the processing is likely to result in a high risk to the rights and freedoms of individuals.
- 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 be 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 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. When using communication technologies, the school considers the following as good practice:

- The official school e-mail service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and pupils should therefore use only the school e-mail service to communicate with others when in school, or on school systems (eg by remote access)

- 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.
- Any digital communication between staff and pupils parents/carers (e-mail, chat, etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal e-mail addresses, text messaging or social media must not be used for these communications.
- Pupils should be taught about online 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 website and only official e-mail addresses, and twitter accounts should be used to identify members of staff.
- When sending emails to multiple recipients outside of the Council, e.g. parents, BCC must be used to avoid sharing of personal email addresses.

Social Media - Protecting Professional Identity

All schools, academies and local authorities have a duty 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 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:
- Expectation of no engagement 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 schools use of social media for professional purposes will be checked regularly by the online safety Subject Leader

Responding to incidents of misuse

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 **Responding to incidents of misuse flowchart** (see appendix) for responding to incidents and report immediately to the police.

Other Incidents

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

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- 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.

Cyber-Bullying

We recognise that children's use of the internet may lead to incidents of cyber-bullying. Cyber-bullying is defined as the use of electronic communication to bully a person and can take many forms. While incidents of cyber-bullying are likely to occur out of school, pupils' online safety lessons are designed to warn them about cyber-bullying, promote respect online and inform them about how to respond to incidents of cyber-bullying. Should staff become aware of incidents of cyber-bullying between pupils, they should adopt a restorative solution approach as outlined in the anti-bullying policy. In addition to this, the parents/carers of the pupils involved will be given information and advice about how to monitor their children's internet use.

Child on child sexual violence and sexual harassment

Sexual violence and sexual harassment can occur between two children of any age and sex, including those of primary school age. They can occur online and face to face (both physically and verbally) and are never acceptable. All staff working with children are advised to maintain an attitude of **'it could happen here.'** Any reported instances of child on child sexual violence or harassment must be reported to the DSL and dealt with in accordance with the safeguarding policy. Should any images be recorded on internet enabled devices, **staff should always avoid viewing them** as to do so would be a criminal offense.

Cybercrime

Cybercrime is criminal activity committed using computers and/or the internet. These include, but are not limited to; unauthorised access to school computers; or making, supplying or obtaining malware with the intent to damage the school network.

Children with particular skill and interest in computing and technology may inadvertently or deliberately stray into cyber-dependent crime.

If there are concerns about a child in this area, the designated safeguarding lead (or a deputy), should consider referring into the **Cyber Choices** programme. This is a nationwide police programme supported by the Home Office and led by the National Crime Agency, working with regional and local policing. It aims to intervene where young people are at risk of committing, or being drawn into, low level cyber-dependent offences and divert them to a more positive use of their skills and interests.

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 an appropriate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures.

Other related policies and relevant documentation

Social media policy

Employee code of conduct

Keeping Children Safe in Education

There is a wealth of information available to support schools and colleges to keep children safe online. The following is not exhaustive but should provide a useful starting point:

www.thinkuknow.co.uk

www.disrespectnobody.co.uk

www.saferinternet.org.uk

www.internetmatters.org

www.childnet.com/cyberbullying-guidance

www.pshe-association.org.uk

educateagainsthate.com

www.gov.uk/government/publications/the-use-of-social-media-for-online-radicalisation

Working together to safeguard children - GOV.UK (www.gov.uk)

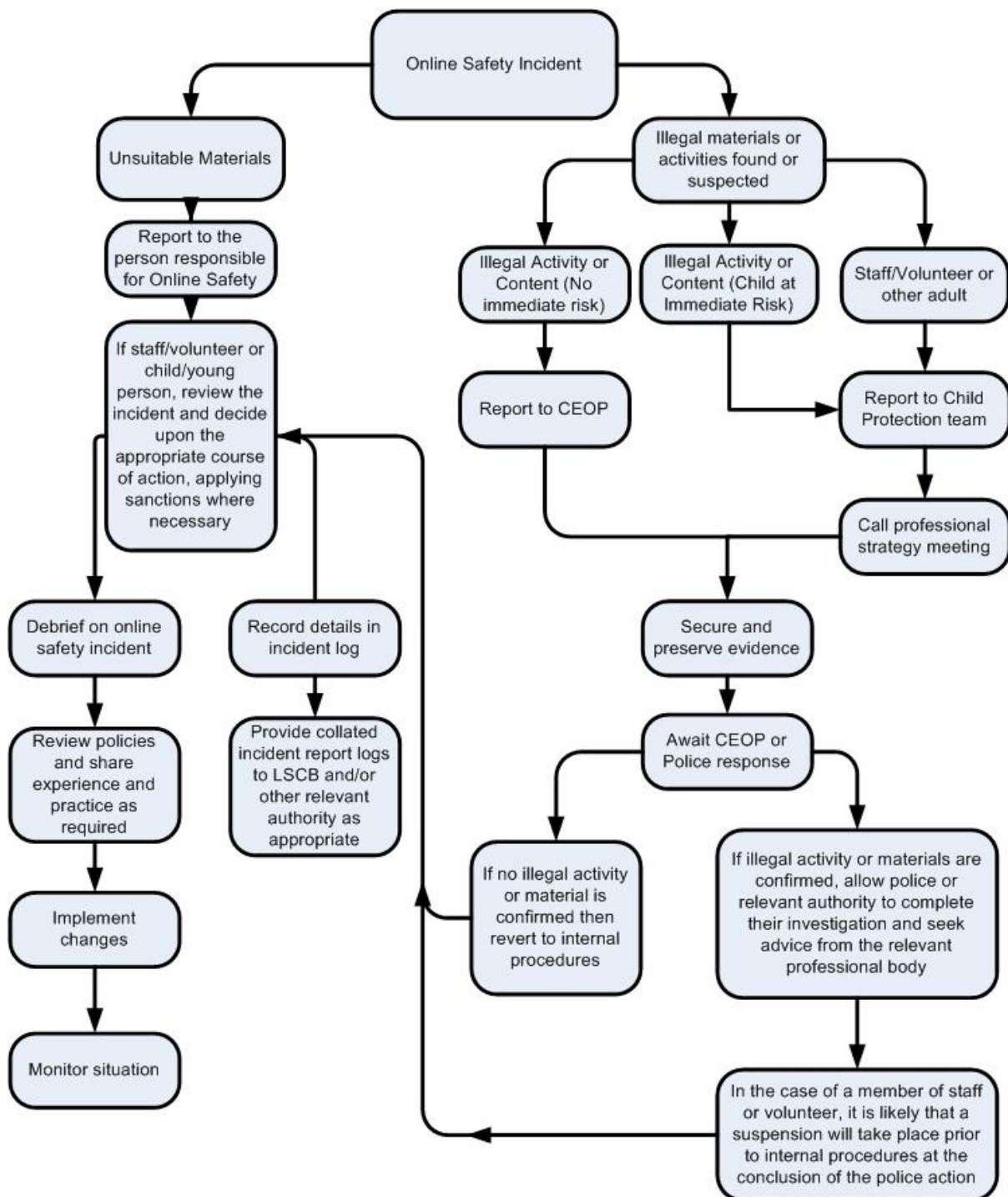
Stat guidance template (publishing.service.gov.uk) (What to do if you're worried a child is being abused.

Sexual violence and sexual harassment between children in schools and colleges - GOV.UK (www.gov.uk)

Appendices

- Responding to incidents of misuse – flowchart
- Record of reviewing sites (for internet misuse)
- School Reporting Log template

Responding to incidents of misuse – flowchart



Record of reviewing devices / internet sites (responding to incidents of misuse)

Group	
Date	
Reason for investigation	

Details of first reviewing person

Name	
Position	
Signature	

Details of second reviewing person

Name	
Position	
Signature	

Name and location of computer used for review (for web sites)

--

Web site(s) address / device

Reason for concern

Conclusion and Action proposed or taken

Reporting Log

Reporting Log Group							
Date	Time	Incident	Action taken		Incident Reported by	Signature	
			What?	By whom?			