Britannica International School, Budapest

A MEMBER OF ARISTON EDUCATION

Online Safety Policy

Approved by:	M W Clack Principal	**Last reviewed on:**	September 2026
Date:	September 2026	**Next review due by:**	August 2027

Development / Monitoring / Review of this Policy

This Online Safety policy has been developed by a committee made up of:

- Principal / Senior Leaders
- Staff – including Teachers, Support Staff, Technical staff
- Director of Education/ Board

Schedule for Development / Monitoring / Review

Item	Detail
This Online Safety policy was approved by the Board	September 2026
The implementation of this Online Safety policy will be monitored by the:	Senior Leadership Team and SLG and PLT and the Network Manager
Monitoring will take place at regular intervals:	Each Year
The Director of Education/ Group Head of IT and the Board will receive a report on the implementation of the Online Safety Policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals:	Annually unless there are incidents of concern which would necessitate an immediate report. Reportable incidents would also be raised in the Principal's Monthly Report.
The Online 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 online safety or incidents that have taken place. The next anticipated review date will be:	August 2027
Should serious online safety incidents take place, the following external persons / agencies should be informed:	Director of Education and the Group Head of IT. Infringement of the law would be referred to the appropriate authority.

The school will monitor the impact of the policy using:

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

Scope of the Policy

This policy applies to all members of the school community (including staff, students, volunteers, parents, visitors, community users) who have access to and are users of school digital technology systems and networks, both in and out of the school.

The school may respond to online conduct occurring outside the site where it affects safeguarding, student welfare, the rights of others, or the orderly operation of the school. Any search, confiscation, examination or deletion involving an electronic device must be lawful, necessary, proportionate and undertaken under an approved school procedure, with safeguarding and data-protection considerations recorded.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents of incidents of any inappropriate Online Safety behaviour that takes place out of school.

Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within the school:

Director of Education acting on behalf of the Board of Directors

The Board is responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Director of Education receiving regular information about online safety incidents and monitoring reports. The Director of Education has taken on the role of Online Safety Operational Board member. The role of the Online Safety Operational Board member will include:

- regular meetings with the Online Safety Officer/ Designated Safeguarding Lead / Principal
- regular monitoring of online safety incident logs
- regular monitoring of filtering / change control logs
- reporting to relevant Board meeting

Principal and Senior Leaders

- The Principal has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the Online Safety Officer (Network Manager).
- The Principal and (at least) one another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. (See flow chart on dealing with online safety incidents).
- The Principal / Senior Leaders are responsible for ensuring that the Online Safety Officer and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The Principal / Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and support those colleagues who take on important monitoring roles.
- The Senior Leadership Team will receive regular monitoring reports from the Online Safety Officer.

Online Safety Officer

- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies / documents

- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- provides training and advice for staff
- where necessary liaises with the municipal authority
- liaises with school technical staff
- receives reports of online safety incidents (via Wellbeing Manager) and creates a log of incidents to inform future online safety developments
- where necessary meets regularly with Online Safety Board members to discuss current issues, review incident logs and filtering / change control logs
- reports regularly to Senior Leadership Team

Network Manager / Technical staff

The Network Manager / Technical Staff / Co-ordinator for ICT / Computing 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 online safety technical requirements and any national /municipal / other relevant body Online Safety Policy / 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 and access is logged.
- that they keep up to date with online safety technical information to effectively carry out their online safety role and to inform and update others as relevant
- that the use of the network / internet / Canvas / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Principal and Online Safety Officer
- that monitoring software / systems are implemented and updated as agreed in school policies

Teaching and Support Staff

Are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current school Online Safety Policy and practices by means of regular training, events or workshops
- they have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP)
- they report any suspected misuse or problem to the Principal / Senior Leader; Online Safety Officer /Designated Safeguarding Lead for investigation / action / sanction
- all digital communications with students and parents should be on a professional level and only carried out using official school systems
- online safety issues are embedded in all aspects of the curriculum and other activities
- they ensure that students understand and follow the Online Safety Policy and acceptable use policies
- Staff ensure that students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies regarding these devices
- in lessons where internet use is pre-planned, students 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

Should be trained in Online Safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

- sharing of any personal data

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

Students

- are responsible for using the school digital technology systems in accordance with the Student Acceptable Use Agreement
- 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 and digital cameras. They should also know and understand policies on the taking / use of images and on online-bullying.
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school

Parents

Parents 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' afternoons, newsletters, letters, website / Canvas, parent workshops and by sharing information about national / local online safety campaigns / literature. Parents will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website / Learning Platform and on-line student records
- their children's personal devices in the school

Community Users

Community Users who access school systems / website / Learning Platform as part of the wider school provision will be expected to sign a Community User AUA before being provided with access to school systems. If third-party contractors have access to school digital resources, no matter how limited, they must also sign an AUA.

Policy Statements

Education – Students

Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students in online safety / digital literacy is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.
Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned online safety curriculum should be provided as part of Computing / PHSE / other lessons and should be regularly revisited

- Key online safety messages should be reinforced as part of a planned programme of tutorial activities
- Students 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.
- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Students should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.
- Students should be helped to understand the need for the student Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school.
- Staff should 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 students 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 students can 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, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

Education – Parents

Many parents have only a limited understanding of online 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 online 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 through:

- Curriculum activities
- Letters, newsletters, web site, Canvas
- Parent workshops
- High profile events / campaigns e.g. Safer Internet Day
- Reference to the relevant web sites / publications e.g. www.saferinternet.org.uk/ http://www.childnet.com/parents-and-carers

Education & Training – Staff / Volunteers

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

- All new staff should receive online safety training (EduCare- Online Safety for International Schools) as part of their induction programme, ensuring that they fully understand the school Online Safety Policy and Acceptable Use Agreements.
- This Online Safety Policy and its updates will be presented to staff in INSET days.
- The Online Safety Officer (or other nominated person) will provide advice / guidance / training to individuals as required.

Training – Director of Education and Board

Board members should take part in online safety training / awareness sessions, with importance for those who are members of any subcommittee / group involved in technology / online safety / health and safety /safeguarding. This may be offered in several ways:

- Training provided by the Group Head of IT
- Participation of online training provided by relevant organisation such as EduCare.
- Participation in school training / information sessions for staff or parents (this may include attendance at assemblies / lessons).

Technical – infrastructure / equipment, filtering and monitoring

The school will be 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. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities:

- 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, network equipment, 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 authorised users will be provided with individual credentials appropriate to their age and role. Password and authentication requirements will follow the school's current technical security standard. Accounts will be disabled promptly when access is no longer required.
- The "master / administrator" passwords for the school ICT systems, used by the Network Manager (or another person) must also be available to the Principal or other nominated senior leader and kept in a secure place (e.g. school safe or preferably in a secure encrypted key vault)
- The Network Manager 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. Illegal content (child sexual abuse images) is filtered by the firewall appliance, broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated, and internet use is logged and regularly monitored.
- Internet filtering / monitoring should ensure that children are safe from radicalisation material when accessing the internet.
- 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 appropriate system (IT helpdesk) is in place for users to report any actual / potential technical incident / security breach to the relevant person.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, workstations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up-to-date anti-virus software.
- An agreed policy is in place for the provision of temporary, time-limited access of "guests" (e.g., trainee teachers, supply teachers, visitors) onto the school systems.
- An agreed policy is in place regarding the extent of personal use that users (staff / students / community users) and their family members are allowed on school devices that may be used out of school.
- An agreed policy is in place that allows staff to / forbids staff from downloading executable files and installing programmes on school devices.

- An agreed policy is in place regarding the use of removable media (e.g. memory sticks / CDs / DVDs) by users on school devices. Personal data cannot be sent over the internet or taken off the school site unless it has been approved, is safely encrypted or otherwise secured.

Mobile Technologies (including BYOD/BYOT)

Mobile technology devices may be school owned/provided or personally owned and might include: smartphone, tablet, notebook / laptop or other technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider internet which may include the school's learning platform and other cloud-based services such as email and data storage.
All users should understand that the primary purpose of the use of mobile / personal devices in a school context is educational. The mobile technologies policy should be consistent with and inter-related to other relevant school polices including but not limited to the Safeguarding Policy, Behaviour Policy, Bullying Policy, Acceptable Use Policy, and policies around theft or malicious damage. Teaching about the safe and appropriate use of mobile technologies is an integral part of the school's Online Safety education programme.
A checklist of points to be considered is included below.

- The school Acceptable Use Agreements for staff, students and parents will consider the use of mobile technologies
- The school allows: (the school should complete the table below to indicate which devices are allowed and define their access to school systems)

Access	School owned (single user)	School owned (multiple users)	Authorised device[1]	Student owned (Y7–13)	Staff owned	Visitor owned
Allowed in school	Yes	Yes	Yes	Yes	Yes	Yes
Full network access	Yes	Yes	No	No	Partial	No
Internet only	No	No	No	Yes – filtered	Yes – filtered	Yes – filtered
No network access	No	No	Yes	Yes	No	Yes

[1] Authorised device – purchased by the pupil/family through a school-organised scheme, or an exam laptop for external exams. This device may be given full access to the network as if it were owned by the school.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents and students 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 about the risks associated with the taking, use, sharing, publication and distribution of images. They should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.

- Written permission from parents will be obtained before photographs of students are published on the school website / social media / local press.
- Parents are welcome to take videos and digital images of their children at school events for their own personal use. 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 comment on any activities involving other students in the digital / video images.
- Staff and volunteers can 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 not remain stored on personal equipment of staff.
- Care should be taken when taking digital / video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Students must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images.
- Students' full names will not be used anywhere on a website or blog, particularly in association with photographs. Student's work can only be published with the permission of the student.

Data Protection

The school will process personal data in accordance with the EU General Data Protection Regulation, applicable Hungarian data-protection law and the school's Data Protection Policy and privacy notices.

Personal data will be recorded, processed, transferred and made available according to the current data protection legislation.

The school must ensure that:

- It has a Data Protection Policy.
- 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.
- Data held must be accurate and up to date. Inaccuracies are corrected without unnecessary delay.
- The lawful basis for processing personal data (including, where relevant, consent) has been identified and documented and details provided in a Privacy Notice.
- Where special category data is processed, a lawful basis and a separate condition for processing have been identified.
- Data Protection Impact Assessments (DPIA) are carried out when introducing new processes or technology to the school that process personal Data.
- It has clear and understood arrangements for access to and the security, storage and transfer of personal data, including, where necessary, adequate contractual clauses or safeguards where personal data is passed to third parties e.g. cloud service providers. A co-signed data handling agreement may be required if data is being accessed or provided to a third-party.
- Procedures must be in place to deal with the individual rights of the data subject i.e. a Subject Access Requests to see all or a part of their personal data held by the data controller.
- There are clear and understood data retention policies and routines for the deletion and disposal of data.
- There is a procedure for reporting, logging, managing and recovering from personal-data incidents, including escalation to the school's data-protection lead and notification to the competent supervisory authority where legally required.
- Consideration has been given to the protection of personal data when accessed using any remote access solutions.
- All staff receive data handling awareness / data protection training and are made aware of their responsibilities.

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. The school considers the benefit of using these technologies for education against their risks and disadvantages, and sets out clear expectations for staff and students on the use of mobile phones, email, messaging apps, social media and blogs, including where use is allowed, restricted to certain times, allowed only for selected/nominated users, or not allowed at all.
When using communication technologies, the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored.
- Users must immediately report, to the DSL 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 students or parents (email, social media, chat, blogs, VLE etc) must be professional in tone and content.
- Students 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 email addresses should be used to identify members of staff.

Social Media - Protecting Professional Identity

With an increase in use of all types of social media for professional and personal purposes a policy that sets out clear guidance for staff to manage risk and behaviour online is essential. Core messages should include the protection of students, the school and the individual when publishing any material online. Expectations for teachers' professional conduct are set out in 'Teachers Standards 2012'. Ofsted's online safety inspection framework and CIS/ COBIS accreditation standards reviews how a school protects and educates staff and students in their use of technology, including the measures that would be expected to be in place to intervene and support should an issue arise. Schools increasingly using social media as a powerful learning tool and means of communication. It is important that this is carried out in a safe and responsible way.
The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm from use of social media to students, staff and the school through:

- Ensuring that personal information is not published

- Training is provided including: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

School staff should ensure that:

- No confidential, private or identifying information about students, parents or colleagues may be posted without an appropriate lawful basis and authorisation.
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school or Ariston Education
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information

When official school social media accounts are established there should be:

- A process for approval by senior leaders
- Clear processes for the administration and monitoring of these accounts – involving at least two members of staff
- A code of behaviour for users of the accounts, including systems for reporting and dealing with abuse and misuse
- Understanding of how incidents may be dealt with under school disciplinary procedures

Personal Use:

- Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy
- Personal communications which do not refer to or impact upon the school are outside the scope of this policy
- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
- The school permits reasonable and appropriate access to private social media sites

Monitoring of Public Social Media

- As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the school
- The school should effectively respond to social media comments made by others according to a defined policy or process

The school's use of social media for professional purposes will be checked regularly by the Online Safety Officer to ensure compliance with the school policies.

Dealing with unsuitable / inappropriate activities

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

The school believes that the following categories of user action would be inappropriate in a school context and that users should not engage in these activities in or outside the school when using school equipment or systems. This includes visiting sites, or making, posting, downloading, uploading, data transferring, communicating or passing on material, remarks, proposals or comments that contain or relate to:

- Child sexual abuse images – unacceptable and illegal (Protection of Children Act 1978)
- Grooming, incitement, arrangement or facilitation of sexual acts against children – unacceptable and illegal (Sexual Offences Act 2003)
- Possession of an extreme pornographic image – unacceptable and illegal (Criminal Justice and Immigration Act 2008)
- Criminally racist material – unacceptable and illegal (Public Order Act 1986)
- Pornography – unacceptable
- Promotion of any kind of discrimination – unacceptable
- Threatening behaviour, including promotion of physical violence or mental harm – unacceptable
- Promotion of extremism or terrorism – unacceptable
- 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 – unacceptable
- Using school systems to run a private business – unacceptable
- Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school – unacceptable
- Infringing copyright – unacceptable
- Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords) – unacceptable
- Creating or propagating computer viruses or other harmful files – unacceptable
- Unfair usage (downloading / uploading large files that hinders others in their use of the internet) – unacceptable
- On-line gaming (educational) – acceptable at certain times
- On-line gaming (non-educational) – acceptable at certain times
- On-line gambling – unacceptable
- On-line shopping / commerce – acceptable at certain times
- File sharing – acceptable at certain times
- Use of social media (see above) – acceptable at certain times
- Use of messaging apps – acceptable at certain times
- Use of video broadcasting e.g. YouTube – acceptable at certain times

Responding to incidents of misuse

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

Illegal Incidents

If illegal child-abuse material or other suspected criminal content is encountered, staff must not view, copy, download, screenshot or investigate it. They must preserve the device and immediately report the matter to the DSL, Principal and police in accordance with the safeguarding incident procedure.

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 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).
- Try to keep a timeline of investigation events as they are carried out, this will make it easier later if a statement of the chain of events is requested by the police.
- 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 internal response or discipline procedures, involvement by the Director of Education/ Group or national / local organisation (as relevant), and/or police involvement and/or action.

If content being reviewed includes images of child abuse, then the monitoring should be halted and referred to the Director of Education and 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
- promotion of terrorism or extremism
- 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 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 safeguarding 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. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures.

Review and Evaluation

This policy is to be reviewed annually, though any deficiencies or weaknesses in arrangements will be remedied without delay.
This policy will be reviewed by the Principal and leadership team. The policy will be reviewed and approved by the Director of Education on behalf of the Board.