# Online Safety Policy
# Hillside Community First School

| | |
|---|---|
| **Adopted date:** | **Spring 2021** |
| **Signature of Headteacher:** | **Jeremy Harrison** |
| **Signature of Governing body:** | **David Morgan** |
| **Next review date** | **Autumn 2023** |

# Scope of the Policy

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

The Education and Inspections Act 2006 empowers Headteachers/Principals to such extent as is reasonable, to regulate the behaviour of students/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 online-bullying or other online safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school/academy.

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 online safety behaviour that take place out of school.

# Roles and Responsibilities

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

# Academy committee members

Academy committee members are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy.

# Headteacher

- The Headteacher 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 Co-ordinator
- The Headteacher and other members 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.
- The Headteacher is responsible for ensuring that the Online Safety Coordinator and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.

# Online Safety Coordinator

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

- 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
- Liaises with DPO in the event of a data breach
- Liaises with the Local Authority
- Liaises with school technical staff
- Receives reports of online safety incidents and creates a log of incidents to inform future online safety developments
- Reports regularly to Senior Leadership Team

## Network Manager

The Network Manager (Academy IT) is responsible for ensuring:

- that the Hillside school's technical infrastructure is secure and is not open to misuse or malicious attack
- that Hillside school's online safety technical requirements are met and any LA Guidance is adhered to.
- that users may only access the networks and devices through a properly enforced password protection policy
- the filtering policy, is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- that they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- that the use of the network, internet, remote access and email is regularly monitored in order that any misuse can be reported to the Headteacher

## Teaching and Support Staff

Are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current Online Safety Policy and practices
- they have read, understood and acknowledged the WAT Responsible Use Policy through myconcern signoff.
- they report any suspected misuse or problem to the Head or Online Safety Coordinator for investigation
- all digital communications with children  and parents or carers should be on a professional level and only carried out using official school systems including online learning platforms such as Dojo, google classrooms etc
- online safety issues are embedded in all aspects of the curriculum and other activities
- children  understand and follow the Online Safety Policy and acceptable use policies

- they monitor the use of digital technologies, mobile devices, cameras in lessons and other school activities and implement current policies with regard to these devices
- in lessons where internet use is pre-planned children 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 Leads

Should be trained in Online Safety issues and be aware of the potential for 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

## Children :

- are responsible for using computers and equipment in accordance with the Pupil Acceptable Use Agreement
- 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
- They should also know and understand policies on the taking and use of images and on cyber-bullying.
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the Online 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. We will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters and the website. Parents and carers 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 (see responsible use policy)

## Education: children

Whilst regulation and technical solutions are very important, their use must be balanced by educating children to take a responsible approach. The education of children in online safety 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 is provided as part of the Computing / and PHSE lessons and should be regularly revisited
- Key online safety messages should be reinforced as part of a planned programme of assemblies
- Children should be taught in all lessons to be critically aware of the materials and content they access on-line and be guided to validate the accuracy of information.
- Children should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Children should be supported in building resilience to radicalisation by providing a safe environment for debating potentially controversial issues and helping them to understand how they can influence and participate in decision-making.
- Children should be helped to understand the need for the student pupil 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 children 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.
- On necessary occasions where older children 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

Many parents and carers 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 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 and the web site, Reference to the relevant web sites / publications*
- *Parents /Carers evenings / sessions online or in person*
- *High profile events / campaigns e.g. Safer Internet Day*

## 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:

- **A planned programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced.**
- **All new staff receive online safety training as part of their induction programme, ensuring that they fully understand the school Online Safety Policy and Responsible Use Agreements and policies.**
- *It is expected that some staff will identify online safety as a training need within the performance management process.*
- *The Online Safety Coordinator (or other nominated person) will receive regular updates through attendance at external training events*
- *This Online Safety Policy and its updates will be presented to and discussed by staff in staff meetings*
- *The Online Safety Coordinator (or other nominated person) will provide advice as required.*

# Training – Governors

**Governors should take part in online safety training or awareness sessions**, with particular importance for those who have responsibility for safeguarding. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority / National Governors Association / or other relevant organisation
- Participation in school information sessions for staff or parents

# Technical – infrastructure / equipment, filtering and monitoring

## Technical – infrastructure/equipment, filtering and monitoring

The school/academy will be responsible for ensuring that the school/academy 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/academy technical systems will be managed in ways that ensure that the school/academy meets recommended technical requirements
- There will be regular reviews and audits of the safety and security of school/academy 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/academy technical systems and devices.
- All users will have a class logon for their class work and accessing the network.
- All users will be provided with a username and secure password by the WAT / school admin for Google classrooms and other online platforms. *Who will keep an up to date record of users and their usernames.* Users are responsible for the security of their username and password.
- The "master/administrator" passwords for the school/academy systems, used by the Network Manager (or other person) must also be available to the *Headteacher* or other nominated senior leader and kept in a secure place (e.g. school/academy safe)

- Finance officer 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 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. There is a clear process in place to deal with requests for filtering changes
- Internet filtering/monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet. N.B. additional duties for schools/academies under the Counter Terrorism and Securities Act 2015 which requires schools/academies to ensure that children are safe from terrorist and extremist material on the internet. (see appendix for information on "appropriate filtering").
- The school/academy has provided enhanced/differentiated user-level filtering (allowing different filtering levels for different ages/stages and different groups of users – staff/pupils/students etc)
- School/academy 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. (schools may wish to add details of the monitoring programmes that are used).
- An appropriate system is in place (to be described) for users to report any actual/potential technical incident/security breach to the relevant person, as agreed).
- Appropriate security measures are in place (schools/academies may wish to provide more detail) 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. These are tested regularly. The school infrastructure and individual devices are protected by up to date virus software.
- An agreed policy is in place for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the school systems. Logon supplied for regular supply teacher and 'supply' limited logon for other supply teachers.
- 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 safely encrypted or otherwise secured.

# Mobile Technologies

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 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, Responsible Use Policy, and policies around theft or malicious damage. Teaching about the safe and appropriate use of mobile technologies should be an integral part of the school's Online Safety education programme. Staff may use personal devices to access learning platforms to check on pupil engagement. Staff must report any inappropriate photographs / videos following the procedures below.

### Parental permission for use of cloud hosted services

Schools/academies that use cloud hosting services are advised to seek appropriate consent to set up an account for learners. Consent for Google Classroom is by accepting an invitation to join.

## Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and children instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and children 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.

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Written permission from parents or carers will be obtained before photographs of children are published on the school website / social media / local press
- 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 children 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 children are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute, parents must be made aware of this when they upload photographs/ video to Google Classrooms.
- Children must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include children 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.

## Data Protection – link to data protection policy WAT

## 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 email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored.
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication
- Any digital communication between staff and children or parents / carers (email, social media, chat, blogs, google classroom, dojo etc) must be professional in tone and content. These communications may only take place on official (monitored) school / academy systems although staff may use personal devices to access the platform. Personal email addresses, text messaging or social media must not be used for these communications.
- Whole class email addresses may be used at KS1, while children at KS2 and above may be provided with group email addresses for educational use. Currently we have do not have email via google classroom.
- Children 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

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

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

- 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 reference should be made in social media to students / pupils, parents / carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community

- Personal opinions should not be attributed to the school or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information

When official school / academy 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 / academy 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 / academy or impacts on the school/ academy, it must be made clear that the member of staff is not communicating on behalf of the school / academy 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

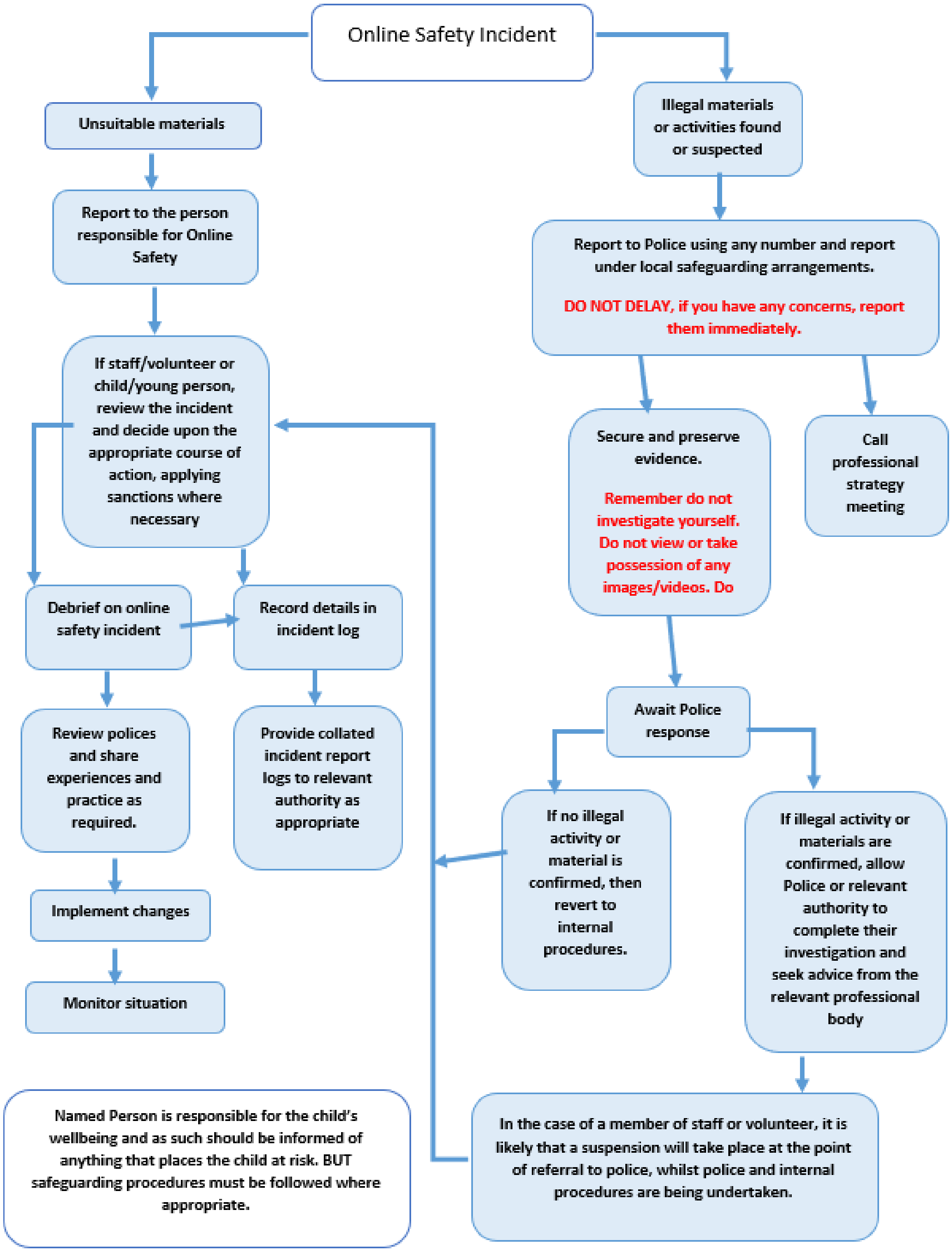
- As part of active social media engagement, Deep South Media pro-actively monitor the Internet for public postings about the school
- The school should effectively respond to social media comments made by others according to a defined process - Deep south media The school's use of social media for professional purposes will be checked regularly by the online safety officer.

# Unsuitable / inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school / academy and all other technical systems. Other activities e.g. cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities. The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in / or outside the school when using school equipment or systems. The school policy restricts usage as follows:

# 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.**: 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.**



Online Safety Incident

Unsuitable materials

Report to the person responsible for Online Safety

If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary

Debrief on online safety incident

Record details in incident log

Review polices and share experiences and practice as required.

Provide collated incident report logs to relevant authority as appropriate

Implement changes

Monitor situation

Illegal materials or activities found or suspected

Report to Police using any number and report under local safeguarding arrangements.

DO NOT DELAY, if you have any concerns, report them immediately.

Secure and preserve evidence.

Remember do not investigate yourself. Do not view or take possession of any images/videos. Do

Call professional strategy meeting

Await Police response

If no illegal activity or material is confirmed, then revert to internal procedures.

If illegal activity or materials are confirmed, allow Police or relevant authority to complete their investigation and seek advice from the relevant professional body

In the case of a member of staff or volunteer, it is likely that a suspension will take place at the point of referral to police, whilst police and internal procedures are being undertaken.

Named Person is responsible for the child's wellbeing and as such should be informed of anything that places the child at risk. BUT safeguarding procedures must be followed where appropriate.

# Other Incidents

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

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

- Have more than one senior member of staff 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/Academy Group 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
    - promotion of terrorism or extremism
    - offences under the Computer Misuse Act (see User Actions chart above)
    - other criminal conduct, activity or materials
- **Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.**

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