

# The Cavendish High Academy



## Online Safety Policy

**2023 - 2024**

## **Reviewed and updated November 2023:**

Donna Tofts  
Online Safety Lead

### **Scope of the Policy**

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

The Education and Inspections Act 2006 empowers Principals to such extent as is reasonable, to regulate the behaviour of students when they are off the academy 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 academy, but is linked to membership of the academy. 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 academy 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 Cavendish High Academy:

#### **Governors**

Governors are responsible for the approval of the online safety policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about online safety incidents and monitoring reports. A member of the Governing Body has taken on the role of Online Safety Governor combined within their role of Safeguarding Governor. The role of the Online Safety Governor/Director will include:

- monitoring of online safety incident logs
- monitoring of filtering/change control logs
- reporting to relevant Governors/Board/Committee/meeting

#### **Principal and Senior Leaders**

Elaine Haver, John Munro, Paula Burke, Clair Ball

- 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 Lead*.
- The Principal and (at least) 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 and Senior Leaders are responsible for ensuring that the Online Safety Lead 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 Headteacher/Principal and 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 also support those colleagues who take on important monitoring roles.*
- *The Senior Leadership Team will receive regular monitoring reports from the Online Safety Lead.*

### **Online Safety Lead**

Donna Tofts

- 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
- 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/ Technical staff**

**Subcontracted to Brindley Data, Mark Poar.**

Those with technical responsibilities are responsible for ensuring:

- that the Academy's technical infrastructure is secure and is not open to misuse or malicious attack
- that the Academy meets required online safety technical requirements and any Local Authority, 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
- 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 networks/internet/digital technologies is regularly monitored in order that any misuse/attempted misuse can be reported to the Online Safety Lead for investigation/action/sanction
- that monitoring software/systems are implemented and updated as agreed in academy 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 academy online safety policy and practices
- they have read, understood and signed the staff acceptable use policy (AUP, Google Form)
- they report any suspected misuse or problem to the Headteacher/Principal/Senior Leader/Online Safety Lead Donna Tofts for investigation/action/sanction
- all digital communications with students/pupils/parents/carers 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
- students understand and follow the Online Safety Policy and acceptable use policies
- 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 with regard to 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**

John Munro, Clair Ball, Paula Burke, Wendy McDonnell

Should be trained in online 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
- online-bullying

### **Students:**

- are responsible for using the academy digital technology systems in accordance to the classroom rules and expected norms
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations through the Computing Curriculum
- 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 *academy's* 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. The academy will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, websites, social media and information about national/local online safety campaigns/literature. Parents and carers will be encouraged to support the academy 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/pupil records
- their children's personal devices in the school/academy (where this is allowed)

### **Policy Statements**

#### **Legislation and guidance**

This policy is based on the Department for Education's statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on preventing and tackling bullying and searching, screening and confiscation. It also refers to the Department's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given

teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

### **Prevent**

The Cavendish High Academy recognises its duty to protect our pupils from accessing terrorist and extremist material on the Internet. The School will therefore aim to do the following:

- Educate pupils on the appropriate use of social media and the dangers of downloading and sharing inappropriate material including that, which is illegal under the Counter- Terrorism Act.
- Ensure that pupils are unable to access any inappropriate Internet sites whilst using the school computers / laptops through the use of appropriate filtering, firewalls and security settings.
- Educate pupils through lessons and assemblies on the concepts of radicalisation and extreme ideology.
- Inform pupils on the importance of Internet Safety both through the ICT curriculum and PSHE education.

### **Education – Students**

Whilst regulation and technical solutions are very important, their use must be balanced by educating students/pupils to take a responsible approach. The education of students in online safety/digital literacy is therefore an essential part of the academy'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.

In planning their online safety curriculum schools may wish to refer to:

- DfE Teaching Online Safety in Schools
- Education for a Connected World Framework
- SWGfL Project Evolve – online safety curriculum programme and resources
- National Online Safety website

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 assemblies and tutorial/pastoral 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.
- Under the Counter Terrorism and Securities Act 2015 requires schools to ensure that students are safe from terrorist and extremist material on the internet.
- 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 the academy.
- 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 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, 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 Mark Poar, Brindley Data 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/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 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/academy will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters, newsletters, web site
- High profile events/campaigns e.g. Safer Internet Day
- Reference to the relevant web sites/publications e.g. [www.swgfl.org.uk](http://www.swgfl.org.uk), [www.saferinternet.org.uk/](http://www.saferinternet.org.uk/), <http://www.childnet.com/parents-and-carers> [www.nationalonlinesafety.com](http://www.nationalonlinesafety.com)

### **Technical – infrastructure/equipment, filtering and monitoring**

The academy will be responsible for ensuring that the 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.

- 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 academy technical systems and devices.
- All users will be provided with a username and secure password. Users are responsible for the security of their username and password.
- The “master/administrator” passwords for the academy systems, used by the Network Manager must also be available to the Principal and kept in a secure place.
- Mark Poar, Brindley Data 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.
- Internet filtering/monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet.
- 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. An appropriate system is in place for users to report any actual/potential technical incident/security breach to the relevant person, as agreed).
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices, etc. from accidental or malicious attempts which might threaten the

security of the school systems and data. These are tested regularly. The school infrastructure and individual devices are protected by up to date virus software.

### **Bark For Schools**

The Cavendish High Academy utilises Bark for Schools, a monitoring system of school-issued G Suite accounts, with specialised extensions for Chrome and Chromebook. Bark for Schools also provides a web filtering feature that allows administration to block and allow domains at the IP and DNS level. Bark for Schools will notify administrators of any content that is deemed as a potential issue. Abuse types included:

- Cyberbullying
- Sexual content
- Depression
- Suicide / self-harm
- Drug related
- Violence
- Hate Speech
- Grooming and Sextortion
- Other (including profanity, drug use, alcohol)

Alerts will be dealt with by Donna Tofts, Online Safety Lead.

### **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/carers and students need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for online-bullying 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. 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 students/pupils 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 academy events for their own personal use (as such use is 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 students in the digital/video images.
- Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow academy policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school/academy equipment; the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital/video images that students/pupils are appropriately dressed and are not participating in activities that might bring the individuals or the academy into disrepute.
- Students/pupils must not take, use, share, publish or distribute images of others without their permission

- Photographs published on the website, or elsewhere that include students 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 students and parents or carers.

### **The use of photographs/video**

- Photographic and video evidence is an integral part of the education and assessment process. Students' photographs and videos are used on a number of internal systems and software for the purpose of student learning. This also includes Earwig for assessment and for the specific gain of accreditations and qualifications with ASDAN and Ascentis.
- Parental consent is gained from all parents/carers in relation to sharing photographic evidence on a number of platforms including the school website, publications and social media.
- Staff should always use a school camera to capture images and should not use their personal devices.
- Photos taken by The Cavendish High academy are subject to the Data Protection Act. Staff should always use a school camera to capture images and should not use their personal devices.
- Photos taken by the school are subject to the Data Protection Act.

### **Data Protection**

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

When personal data is stored on any mobile device or removable media the:

- data must be encrypted and password protected.
- device must be password protected.
- device must be protected by up to date virus and malware checking software
- data must be securely deleted from the device, in line with academy policy once it has been transferred or its use is complete.

Staff must ensure that they:

- at all times take care to ensure the safekeeping of personal data, minimising the risk of its loss or misuse
- can recognise a possible breach, understand the need for urgency and know who to report it to within the school
- can help data subjects understand their rights and know how to handle a request whether verbal or written. Know who to pass it to in the school
- where personal data is stored or transferred on mobile or other devices (including USBs) these must be encrypted and password protected.
- will not transfer any academy personal data to personal devices except as in line with school policy
- access personal data sources and records 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



## Communications

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

When using communication technologies, the academy considers the following as good practice:

- The official school/academy email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and students should therefore use only the academy email service to communicate with others when in school, or on academy systems (e.g. by remote access).
- Users must immediately report, to the nominated person – in accordance with the academy 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 students or parents (email) must be professional in tone and content. These communications may only take place on official (monitored) academy systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Personal information should not be posted on the academy website and only official email addresses should be used to identify members of staff.

## Social Media - Protecting Professional Identity

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

The academy 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

Academy staff should ensure that:

- No reference should be made in social media to students, parents/carers or academy 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 *academy* or local authority/MAT
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information

When official 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 personal social media accounts. In all cases, where a personal account is used which associates itself with the academy or impacts on the academy, it must be made clear that the member of staff is not communicating on behalf of the 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 academy 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 proactively 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 Cavendish High Academy is in partnership with Halton Association of Secondary Headteachers supporting a Social Media Code of Conduct for Parents/Carers.**

Halton Association of Secondary Headteachers understand the benefits of using social media. However, if misused it can be extremely detrimental to our young people, staff and school communities.

The purpose of this code of conduct is to provide clear guidelines on how we expect other relevant parties (guardians) to conduct themselves on social media and when using messenger apps such as WhatsApp, to avoid the negative impacts misuse can have. The Social Media Code of Conduct for parents/carers sits alongside and compliments the social media expectations for both staff and students.

The Halton Association of Secondary Headteachers are aware of their obligations under this code of conduct and ask that parents and carers support their child's secondary school to ensure students, staff and other members of the school community are further protected.

**Google Classroom in the GSuite for Education**

The Cavendish High Academy has adapted G Suite for Education - a set of productivity tools from Google including Gmail, Calendar, Docs, Classroom and more. Students will use their G Suite accounts to complete tasks, evidence learning, communicate with their teachers and learn 21st century digital citizenship skills.

Students use a Gmail login to access the school system servers and the internet. All email addresses are created by G Suite admin and will be within the school domain @chs.academy. Google Cloud does contain electronic work students complete.

Google's Privacy Policy for GSuite;

[https://workspace.google.com/terms/education\\_privacy.html](https://workspace.google.com/terms/education_privacy.html)

<https://edu.google.com/why-google/privacy-security/>

[https://workspace.google.com/intl/en/terms/education\\_terms.html](https://workspace.google.com/intl/en/terms/education_terms.html)

For further information on the use of Google’s G Suite for Education please contact Donna Tofts.

**Visitors and members of the community**

Visitors and members of the community who use the school’s ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use.

**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 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/academy context, either because of the age of the users or the nature of those activities.

The academy believes that the activities referred to in the following section would be inappropriate in an academy context and that users, as defined below, should not engage in these activities in/or outside the school/academy when using academy equipment or systems. The academy policy restricts usage as follows:

**Student Actions**

		Acc ept abl e	Acc ept abl e at cer tai n tim es	Acc ept abl e for no mi nat ed use rs	Un acc ept abl e	Un acc ept abl e and ille gal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material,	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	Pornography				X	

remarks, proposals or comments that contain or relate to:	Promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	Promotion of extremism or terrorism				X	
	Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Activities that might be classed as cyber-crime under the Computer Misuse Act:						
<ul style="list-style-type: none"> <li>Gaining unauthorised access to school networks, data and files, through the use of computers/devices</li> <li>Creating or propagating computer viruses or other harmful files</li> <li>Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)</li> <li>Disable/Impair/Disrupt network functionality through the use of computers/devices</li> <li>Using penetration testing equipment (without relevant permission)</li> </ul>						X
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school/academy					X	
Revealing or publicising confidential or proprietary information (e.g. financial/personal information, databases, computer/network access codes and passwords)					X	
Unfair usage (downloading/uploading large files that hinders others in their use of the internet)					X	
Using school systems to run a private business					X	
Infringing copyright					X	
On-line gaming (educational)		X				
On-line gaming (non-educational)		X				
On-line gambling					X	
On-line shopping/commerce		X				
File sharing		X				
Use of social media					X	
Use of messaging apps					X	
Use of video broadcasting e.g. Youtube						
		X				

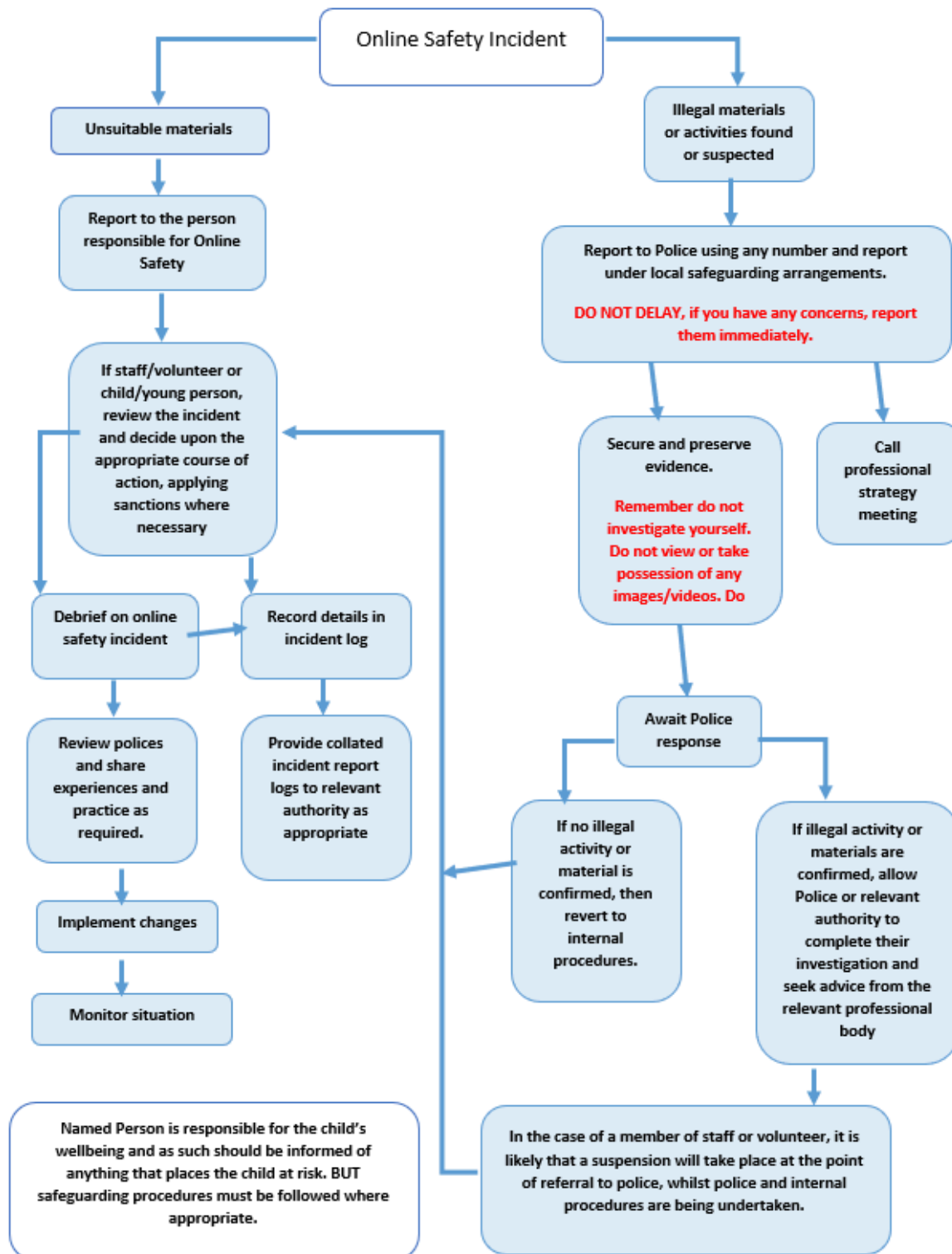
**Responding to incidents of misuse - Staff Acceptable Use Policy**

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 there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the police.



## Other Incidents

It is hoped that all members of the 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 *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.



