# Hayle Academy

## ONLINE SAFETY POLICY

**School Name:** Hayle Academy
**Dissemination:** Website and T: Drive
**Date policy approved by Governors:** February 2024
**Date policy becomes effective:** Immediately
**Review date:** February 2026
**Person responsible for Implementation and Monitoring:** Headteacher, DSL
**Links to other relevant policies:** Safeguarding, Anti-Bullying, ICT Acceptable Use, Banned Substances, Student Behaviour, GDPR, Disciplinary

### Scope of the Policy

This policy applies to all members of Hayle Academy (including staff, students, 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 Headteachers 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 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 Governing Body receiving regular information

about online safety incidents and monitoring reports, as a routine part of the monitoring of safeguarding. A member of the Governing Body has taken on the role of Safeguarding Governor, which will include:

- regular meetings with the Online Safety Lead (DSL) to review:
    - meetings of the IT Safety Group
    - monitoring of online safety incident logs
    - monitoring of filtering/change control logs
- reporting to relevant Governors' Meetings

## Headteacher and Senior Leaders

- 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 Lead.
- The Headteacher, Deputy Headteacher and Designated Safeguarding Lead are 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 – included in a later section – "Responding to incidents of misuse" and relevant procedures).
- The Headteacher 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 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 to those colleagues who take on important monitoring roles, as part of regular safeguarding meetings and, where appropriate, supervision.
- The Senior Leadership Team will receive regular monitoring reports from the Online Safety Lead.

## Online Safety Lead (DSL)

- The Online Safety Lead will be the Designated Safeguarding Lead. The DSL:
    - 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 TPAT with regards to online safety
    - liaises with IT technical staff
    - receives reports of online safety incidents and ensures there is a log of incidents to inform future online safety developments, via CPOMs
    - meets regularly (minimum termly) with the Safeguarding Governor to discuss current issues, review incident logs and filtering/change control logs
    - attends relevant meetings of Governors
    - reports regularly to the Senior Leadership Team
- The DSL is aware of the potential for serious child protection and safeguarding issues to arise from:

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

## Network Manager/Technical staff

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 Trust online safety policy/guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy
- that 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 Academy network, internet and digital technologies is regularly monitored in order that any misuse or attempted misuse can be reported to the Senior Leadership Team or DSL for investigation, action and sanction
- that monitoring software and 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)
- they report any suspected misuse or problem to the Senior Leadership Team or DSL for investigation, action and sanction
- all digital communications with students and parents/carers are on a professional level and only carried out using official school systems
- online safety issues are embedded where appropriate 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 are 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

## IT Safety Group

The IT Safety Group provides a consultative group that has wide representation from the Academy community, with responsibility for issues regarding online safety and the monitoring of the Online Safety Policy including the impact of initiatives.

Members of the IT Safety Group will assist the Online Safety Lead with:

- the production, review and monitoring of the school online safety policy.
- the production, review and monitoring of the school filtering policy and requests for filtering changes.
- mapping and reviewing the online safety and digital literacy curricular provision – ensuring relevance, breadth and progression
- consulting stakeholders – including parents/carers and students - about online safety
- discuss safeguarding and the IT systems including hardware, data storage and transfer

## Students:

- are responsible for using the Academy digital technology systems in accordance with the student acceptable use agreement
- are taught to have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- are taught to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- are expected to know, understand and follow Academy policies on the use of school IT systems, internet, mobile devices and digital cameras. They should also know, understand and follow Academy policies on the taking and use of images and online-bullying.
- are expected to 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 Academy IT systems, internet and mobile devices in an appropriate way. The Academy will use opportunities to help parents understand these issues e.g. through parents' evenings, newsletters, letters, website, social media and information about national and local online safety literature. Parents and carers are expected 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 and remote Learning Platform and on-line student records

### Community Users

Community Users who access Academy systems or programmes as part of the wider Academy provision will be expected to sign and follow an AUP before being provided with access to Academy systems.

# 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 and digital literacy is therefore an essential part of the Academy's online safety provision. Students need the help and support of the school to recognise and avoid online safety risks and build their resilience.

Online safety is a focus in all areas of the curriculum where appropriate and staff reinforce online safety messages across the curriculum. The online safety curriculum is broad, relevant and provides progression, with opportunities for creative activities and will be provided in the following ways:

- A planned online safety curriculum will be provided as part of Computing and Global Values lessons and will be regularly revisited
- Key online safety messages are reinforced as part of a planned programme of assemblies and tutorial activities
- Students are taught in lessons to be critically aware of the materials and content they access on-line and are guided to validate the accuracy of information.
- Students are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Students are 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 are helped to understand the need for the student acceptable use agreement (AUP) and encouraged to adopt safe and responsible use both within and outside the Academy.
- Staff are expected to 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 are 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 are expected to be vigilant in monitoring the content of the websites that students 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 temporarily remove those sites from the filtered list for the period of study. Any request to do so will be logged and monitored with clear reasons for the need.

## Education – Parents/carers

Some parents and carers may 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 and 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 Academy will therefore seek to provide information and awareness to parents and carers through:

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

## Education – The Wider Community

From time to time the Academy may provide opportunities for local community groups and members of the community to gain from the Academy's online safety knowledge and experience. This may be offered through the following:

- Providing family learning courses in use of new digital technologies, digital literacy and online safety
- Online safety messages targeted towards grandparents and other relatives as well as parents.
- The Academy website will provide online safety information for the wider community
- Sharing online safety expertise and good practice with other local schools
- Supporting community groups e.g. Early Years Settings, Childminders, youth/sports/voluntary groups to enhance their online safety provision Education & Training

## Training – Staff

Staff will receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- Annual training for all staff updating on online safety, including distribution of this online safety policy and any updates.
- All new staff will receive online safety training as part of their induction programme, ensuring that they fully understand the Academy online safety policy and AUPs**.**
- It is expected that some staff may identify online safety as a training need within the performance management process.
- The DSL will receive regular updates through attendance at external training events (e.g. from SWGfL/LA/other relevant organisations) and by reviewing guidance documents released by relevant organisations.
- The Online Safety Lead (or other nominated person) will provide advice, guidance and training to individuals as required.

## Training – Governors

**Governors will take part in online safety training sessions**, alongside their safeguarding training, with particular importance for those who have a role in technology, online safety, health and safety and safeguarding. This training and support may be offered in a number of ways:

- Attendance at training provided by the Local Authority, TPAT, National Governors Association, or other relevant organisation (e.g. SWGfL).
- Participation in Academy training and information sessions for staff or parents
- Training provided as part of Governors' Meetings

## Technical – infrastructure/equipment, filtering and monitoring

Hayle Academy, as part of Truro and Penwith Academy Trust (TPAT) receives technical support from a central Trust IT Support Team. This team are aware of the technical requirements and policies of Hayle Academy as well as local and national requirements and best practice for use of infrastructure, equipment, filtering and monitoring.

## 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 will inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular, they will be supported to 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 are published on the school website, social media and/or local press
- Staff and volunteers are allowed to take digital or video images to support educational aims, and must follow Academy policies concerning the sharing, distribution and publication of those images. Those images should only be taken on Academy equipment; the personal equipment of staff should not be used for such purposes.

- Care should be taken when taking digital or video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the Academy into disrepute.
- Students must not take, use, share, publish or distribute images of others without their permission. Children under the age of 12 are not generally considered able to provide informed consent. Therefore, students must not take, use, share or publish or distribute images of other students in Year 7 or 8 unless express permission to do so has been given by a parent or member of staff.
- 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 will only be published with the permission of the student and parents or carers.

### Data Protection

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

## Communications

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

- The official Academy email service is 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 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/carers (email, social media, chat, blogs, VLE etc) 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.

### Social Media - Protecting Professional Identity

All schools, MATs and local authorities have a duty of care to provide a safe learning environment for students and staff. Schools, 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 Academy or Trust 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 will ensure that:

- No reference is 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 are not to be attributed to the Academy or Trust
- 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 must be:

- Approval by the Headteacher
- 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 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 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 Academy 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.

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 Academy will effectively and appropriately respond to social media comments made by others according to a defined policy or process
- The Academy's use of social media for professional purposes will be checked regularly by the Senior Leadership Team to ensure compliance with Academy policies.

# Managing unsuitable/inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and is obviously banned from the Academy and all other technical systems. Other activities e.g. cyber-bullying are also 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 Academy believes that the activities referred to in the following section are inappropriate in a school context and that users, as defined below, should not engage in these activities in or outside the Academy when using Academy equipment or systems. The Academy policy restricts usage as follows:

| User Actions | | Acceptable | Acceptable at certain times | Acceptable for nominated users | Unacceptable | Unacceptable and illegal |
|---|---|---|---|---|---|---|
| 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 |

| | | | | | | |
|---|---|---|---|---|---|---|
| remarks, proposals or comments that contain or relate to: | Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986 | | | | | X |
| | Pornography | | | | X | |
| | Promotion of any kind of discrimination | | | | X | |
| | threatening behaviour, including promotion of physical violence or mental harm | | | | X | |
| | 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:<br>● Gaining unauthorised access to school networks, data and files, through the use of computers/devices<br>● Creating or propagating computer viruses or other harmful files<br>● Revealing or publicising confidential or proprietary information (e.g. financial or personal information, databases, computer or network access codes and passwords)<br>● Disable/Impair/Disrupt network functionality through the use of computers/devices<br>● Using penetration testing equipment (without relevant permission) | | | | | | X |
| Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the 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 | |

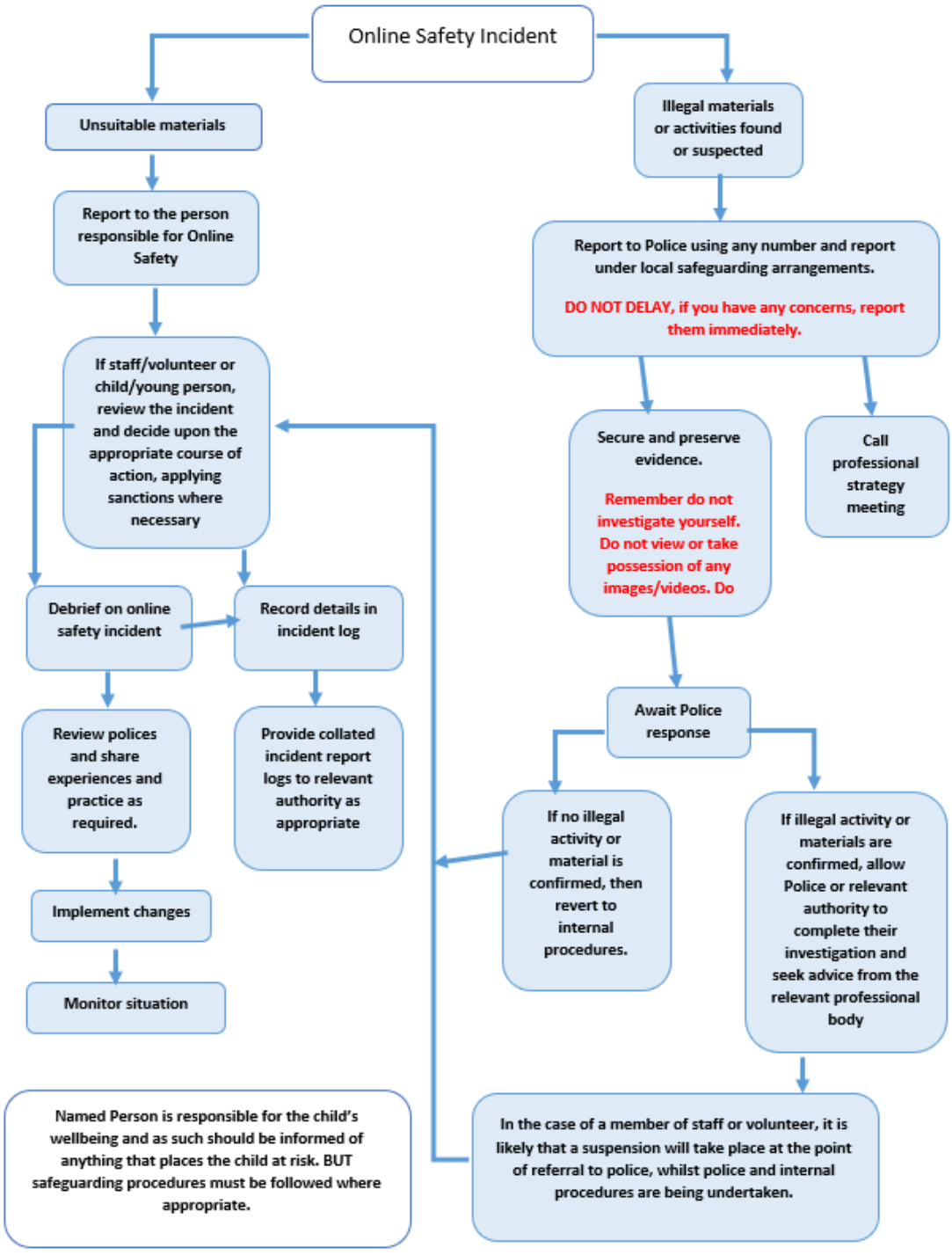
| | | | | | |
|---|---|---|---|---|---|
| On-line shopping/commerce | | | X | | |
| File sharing | | | X | | |
| Use of social media | | | X | | |
| Use of messaging apps | | | X | | |
| Use of video broadcasting e.g. Youtube | | | X | | |

# Responding to incidents of misuse

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 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
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.
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.

## Other Incidents

It is hoped that all members of the Academy community will be responsible users of digital technologies, who understand and follow 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 a concern, all steps in this procedure should be followed:**

- At least two members of staff (including one senior leader) will be 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 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.
- 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 of the Trust or national/local organisations (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 far as possible. 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.

# Academy actions & sanctions

It is more likely that the Academy 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 and disciplinary procedures linked to the relevant policies.

# Digital Transformation

The ultimate aim of our schools is to improve outcomes and opportunities for our young people, and to help prepare them for the future. In order to support this, we are joining the TPAT Advantage program to give our teachers and pupils the very best digital tools available to support them in their work and to enhance their learning. In order to support students to stay safe online, we have put in place advanced and secure filtering and monitoring systems through Netsweeper, which enables us to monitor and control all internet use on the iPads, even when the device is being used at home. Monitoring of this will support in identifying any further training or safety measures that may be required as the technology evolves. Robust training and support plans are in place for staff and students. An acceptable user policy is in place for the use and deployment of the iPads, which is shared with parents/carers. The camera roll on the iPads will be subject to spot checks and monitoring through a range of measures, including SLT visits to tutor rooms.