Gladstone Primary
Academy

TDET
Thomas Deacon Education Trust

Policy:	Online Safety
Owner:	Paul Fountain
Approving Board:	Academy Committee
Date of review:	May 2022
Date of next review:	May 2023
Publish Status:	Approved
Version:	1

Aims

The Online Safety Policy aims to outline safe, risk free and effective practice to ensure we provide Online Safeguarding to meet the needs of all users. It provides advice on acceptable use and effective measures to enable children, young people and adults to use ICT resources in a safer online environment. This policy will be reviewed regularly to ensure we adjust to meet new challenges which may arise or will be examined immediately if there is a major online safety incident.

Scope

This policy applies to all members of the Academy including Academy Committee members, staff, pupils, volunteers, parents or carers, contractors, supply staff and visitors who have access to and are users of Academy ICT systems, both in and out of the Academy.

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education 2022, and its advice for Academies on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying:

  advice for headteachers and school staff

- Relationships and sex education
- Searching, screening and confiscation

It also refers to the Department's guidance on protecting children from radicalisation. The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the Academy's premises and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyberbullying or other Online Safety incidents covered by this policy, which may take place outside of the Academy, but is linked to pupils 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 and the updated Searching Screening and Confiscation Policy 2018. The Academy will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents or carers of incidents of inappropriate Online Safety behaviour that take place out of the Academy. The policy also takes into account the National Curriculum computing programmes of study and the requirements of the Equality Act 2010.

Roles and Responsibilities

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

Academy Committee members:

Academy Committee members 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 Academy Committee receiving regular information about online safety incidents and monitoring reports. A member of the Academy Committee has taken on the role of Online Safety Academy Committee member (this will usually be the same member for safeguarding). The role of the Online Safety Academy Committee member will include:

- regular meetings with the ICT Lead
- attendance at Online Safety Group meetings
- regular monitoring of online safety incident logs
- regular monitoring of filtering / change control logs
- reporting to relevant Academy Committee meeting

Headteacher / Senior Leadership Team (SLT):

- The Headteacher has a duty of care for ensuring the safety, including online safety of members of the Academy community.
- The Headteacher and 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 and SLT are responsible for ensuring that the ICT 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 and SLT will ensure that there is a system in place to allow for monitoring and support of those in the Academy 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. The 360 degree monitoring tool will be completed.
- The SLT will receive regular monitoring reports from the Online Safety Coordinator.

Online Safety Lead:

- leads the Online Safety Group
- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the Academy 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 the Local Authority / relevant body
- liaises with Academy technical staff
- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments

- meets regularly with Online Safety Academy Committee member to discuss current issues, review incident logs and filtering / change control logs
- attends relevant meetings of the Academy Committee
- reports regularly to Senior Leadership Team

Technical staff:

Gladstone Primary Academy receives technical support as a member of the Thomas Deacon Education Trust, it is the responsibility of the Academy to monitor and ensure TDET follow the Academy's Online Safety Policy and procedures.

The Technical Staff is 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 that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- the filtering policy supplied by E2BN 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 and attempted misuse can be reported to the Headteacher, SLT and Online Safety Coordinator for investigation and action.
- 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's 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 Headteacher or SLT for investigation and action.
- all digital communications with students / pupils / parents / carers should be on a professional level and only carried out using official Academy systems
- online safety issues are embedded in all aspects of the curriculum and other activities
- pupils understand and follow the Online Safety Policy and acceptable use policies
- pupils 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 Academy activities (where allowed) and implement current policies with regard to these devices
- in lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Designated Safeguarding Lead

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

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

The DSL logs behaviour and safeguarding issues related to online safety. The on-line platform My Concern is used to log these incidents.

Online Safety Group:

The Online 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. Depending on the size or structure of the Academy this group may be part of the safeguarding group. The group will also be responsible for regular reporting to the Academy Committee. Members of the Online Safety Group will assist the Online Safety Coordinator with:

- the production / review / monitoring of the Academy Online Safety Policies.
- the production / review / monitoring of the Academy filtering policy
- mapping and reviewing the online safety curricular provision – ensuring relevance, breadth and progression
- monitoring network / internet / incident logs
- consulting stakeholders – including parents and carers and pupils about the online safety provision
- monitoring improvement actions
- Digital Leaders will also be part of the Online Safety Group.

Pupils:

- are responsible for using the Academy digital technology systems in accordance with the Pupil Acceptable Use Agreement

- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking and use of images and on cyber-bullying.
- should understand the importance of adopting good online safety practice when using digital technologies out of the Academy and realise that the Academy's Online Safety Policy covers their actions out of the Academy, if related to their membership of the Academy

Parents and Carers

Parents and Carers play a crucial role in ensuring that their children understand the need to use the internet and mobile devices in an appropriate way. The Academy will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website, family cafes and information about national and local online safety campaigns. 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 Academy events
- access to parents' sections of the website and online pupil records, such as Tapestry
- their children's personal devices in the Academy

Policy Statements

Education – Pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety is therefore an essential part of the Academy's online safety provision. Children and young people need the help and support of the Academy to recognise and avoid online safety risks and build their resilience.

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

- A planned online safety curriculum should be provided as part of 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
- pupils should be taught in all lessons to be critically aware of the content they access online and be guided to validate the accuracy of information.
- pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- pupils 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.
- pupils should be helped to understand the need for the pupil 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 pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet they should use Safe Search or Swiggle and 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 (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff 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. Pupils should be guided towards age appropriate content.

Education – Parents and 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 of their 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:

- Curriculum activities
- Letters, newsletters, web site,
- Parents / Carers evenings or sessions
- High profile events and campaigns such as Safer Internet Day

Education – The Wider Community

The Academy will provide opportunities for local community to gain from the Academy's online safety knowledge and experience. This may be offered through the following:

- Online safety messages targeted towards grandparents and other relatives as well as parents.
- The Academy will provide online safety information for the wider community to access via the website and parent mail.

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. An audit of the online safety training needs of all staff will be carried out regularly. All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the Academy Online Safety Policy and Acceptable Use Agreements. It is also expected that some staff will identify online safety as a training need within the performance management process.
- The Online Safety Coordinator will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.
- This Online Safety Policy and its updates will be presented to and discussed by staff in staff meetings or INSET days.
- The Online Safety Lead will provide advice and training to individuals as required.

Training – Academy Committee

Academy Committee members should take part in online safety training, with particular importance for those who are lead Academy Committee members involved in technology, online safety, health and safety or safeguarding. This may be offered in several ways:

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

Technical – infrastructure / equipment, filtering and monitoring

Thomas Deacon Education Trust ICT service follow policies set by Gladstone Primary Academy and Trust to ensure that all safe practices are adhered to.

The Academy will be responsible for ensuring that the Academy infrastructure and 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:

- Academy technical systems will be managed in ways that ensure that the Academy meets recommended technical requirements
- There will be regular reviews and audits of the safety and security of 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.
- Staff are responsible for keeping their passwords safe and ensure they are regularly updated. All ICT users should have strong passwords.
- The "master / administrator" passwords for the Academy ICT system, must also be available to the Headteacher and kept in a secure place (eg safe)
- The Online Safety Lead 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 licenses purchased against the number of software installations. Inadequate licensing could cause the Academy to breach the Copyright Act which could result in fines or unexpected licensing costs.
- Internet access is filtered for all users. Illegal content (for example, child sexual abuse images) is filtered by the broadband or filtering provider E2BN 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 whereby the Online Safety Lead or Headteacher/SLT will contact E2BN via TDET ICT support and this will be recorded on the filtering change log.
- Internet filtering 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 Academy 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 Head Teacher or SLT as described in the ICT Acceptable Use Policy.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, workstations, mobile devices etc from accidental or malicious

attempts which might threaten the security of the Academy systems and data. These are tested regularly.

- The Academy infrastructure and individual workstations are protected by up to date virus software.
- The Server Room is locked with limited access and back up procedures are in place.
- An agreed policy is in place for the provision of temporary access of “guests” (eg trainee teachers, supply teachers, visitors) onto the Academy systems.
- Staff should take necessary steps to ensure the safe use of Academy devices that may be used out of the Academy. Devices should be kept secure, not used in public places and with strong passwords/pin codes set up. If a device is lost the Headteacher or SLT should be notified immediately to assess if there may be a potential data breach.
- Staff cannot download executable files and install programs on Academy devices without being checked by the TDET ICT Technician.
- The Academy policy is that removable media are not to be used (e.g. memory sticks). One Drive is the platform for accessing data when not at the Academy or for sharing with other members of staff.

Filtering and Monitoring

Internet Filtering

To ensure a safe online environment, Gladstone Primary Academy through Thomas Deacon Education Trust will implement appropriate internet filtering systems. These systems will be regularly updated to block access to inappropriate and harmful content. The filtering will cover all internet-connected devices within the organization's network, including desktop computers, laptops, tablets, and mobile devices.

Monitoring and Reporting

Gladstone Primary Academy through Thomas Deacon Education Trust will monitor online activities within the organization's network to identify any misuse, inappropriate content, or potential safeguarding concerns. Monitoring will be conducted in a proportionate and transparent manner, ensuring the privacy of individuals is respected. If any concerns are identified, they will be reported by the TDET IT team to the Online Safety Coordinator (who must be a trained DSL) for appropriate action.

Mobile Technologies (including BYOD/BYOT)

Mobile technology devices may be Academy provided or personally owned and might include: smartphone, tablet, notebook / laptop or other technology that usually has the capability of utilising the Academy's wireless network. The device then has access to the wider internet which may include 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 the Academy context is educational. The mobile technologies policy should be consistent with and inter-related to other relevant Academy policies including but not limited to the Safeguarding Policy, Behaviour Policy, Bullying Policy, Acceptable Use Policy, and policies around theft or malicious damage. Teaching about the safe and appropriate use of mobile technologies should be an integral part of the Academy's Online Safety education programme.

- The Academy Acceptable Use Agreements for staff, pupils and parents/carers will give consideration to the use of mobile technologies.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents or carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The Academy will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm. If an image is inadvertently uploaded Gladstone Primary Academy will remove as soon as the error has been identified.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018 and in accordance with GDPR 2018 which states that personal data must be:

- Processed lawfully
- For a specific purpose
- Kept to a minimum
- Accurate and up to date
- Retained only for as long as needed
- Kept securely

The Academy must ensure that:

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- All personal data will be fairly obtained in accordance with the “Privacy Notice” and lawfully processed in accordance with the “Conditions for Processing”. It has a GDPR/Data Protection Policy.
- It is registered as a Data Controller.
- Responsible persons are appointed to ensure that data is kept securely at Gladstone Primary Academy.
- Risk assessments are carried out
- It has clear and understood arrangements for the security, storage and transfer of personal data.
- Data subjects have rights of access and there are clear procedures for this to be obtained.
- There are clear and understood policies and routines for the deletion and disposal of data.
- There is a policy for reporting, logging, managing and recovering from information risk incidents
- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties.
- There are clear policies about the use of cloud storage / cloud computing which ensure that such data transfer / storage meets the requirements laid down by the Information Commissioner’s Office.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly “logged-off” at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.

When personal data is stored on any portable computer system or any removable media:

- the data must be encrypted and password protected
- The device must be password protected
- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device, in line with Academy policy once it has been transferred or its use is complete.

Please refer to the Academy policy on Data Protection/GDPR

Online Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning.

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

- The official Academy email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and pupils should therefore use only the Academy email service or Offive 365 to communicate with others when in the Academy or on Academy premises.
- Users must immediately report, to a member of staff if they receive any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and pupils 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 Academy systems. 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 pupils at KS2 and above will be provided with individual Academy email addresses for educational use.
- Students / pupils should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies. If they bring in a mobile device into the Academy it should be handed into the Academy office during the Academy day and returned to the pupil at 3pm.
- 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 and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the Academy, the Academy Trust, or local authority 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 Academy 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 pupils, parents, carers or Academy staff
- They do not engage in online discussion on personal matters relating to members of the Academy community
- Personal opinions should not be attributed to the Academy or local authority
- 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 academy disciplinary procedures

Personal Use:

- Personal communications are those made via a personal social media account. 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 the Academy 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 pro-actively monitor the Internet for public postings about the Academy
- The Academy should effectively 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 SLT and Online Safety Group to ensure compliance with the Academy policies.

Unsuitable / inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from the 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. Please refer to the Acceptable Use, Code of Conduct and Safeguarding Policies for guidance.

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 Headteacher immediately and report immediately to the police.

Other Incidents

Academy staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- ➢ Cause harm, and/or
- ➢ Disrupt teaching, and/or
- ➢ Break any of the Academy rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of Academy discipline), and/or
- Report it to the police

Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation.

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the Academy's complaints procedure.

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 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:

    o Internal response or discipline procedures

    o Involvement by Local Authority

    o 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:

o adult material which potentially breaches the Obscene Publications Act

o criminally racist material o promotion of terrorism or extremism

o 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.

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 Academy 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.

This policy should be read in conjunction with:

Child protections and safeguarding policy

Behaviour policy

Acceptable use policy

Staff code of conduct

Review

This policy will be reviewed annually by the online safety lead.