Langley Hall Arts Academy

SSPo24

# E-SAFETY POLICY

| POLICY | PROCEDURE | REFERENCE | FORMS |
|---|---|---|---|
| SSPo42 GDPR Policy | | Data Protection Act 1998 | |
| SSPo2 Child Protection and Safeguarding Children Policy and Procedure | | Education Act 2011 | |
| | | Education and Inspections Act 2006<br>Data Protection Policy<br>Privacy Notices<br>Complaints and Concerns Policy | |

## About the Policy

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

This policy should also be read alongside the Child Protection and Safeguarding Children Policy and Procedure, the Data Protection Policy, Privacy Notices, Complaints and Concerns Policy, Cybersecurity and IT Acceptable Use procedures and any guidance relating to artificial intelligence and generative AI. The Academy recognises that cybersecurity is not solely a technical or operational matter. In accordance with Keeping Children Safe in Education, cybersecurity forms part of the school's safeguarding responsibilities because weaknesses in cyber security may expose children and adults to harm through data breaches, loss of safeguarding information, online exploitation, harmful content, fraud, impersonation, disruption of essential systems or other risks affecting welfare and safety.

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 school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The Education Act 2011 increased these powers with regard to the searching for and of electronic devices and the deletion of data (see appendix for policy. The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school.

## Roles and Responsibilities

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

### Governors

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about e-safety

 © Langley Hall Arts Academy 2022

incidents and monitoring reports. A member of the Governing Body has taken on the role of E-Safety Governor. The role of the E-Safety Governor will include:

- regular meetings with the E-Safety Co-ordinator
- regular monitoring of e-safety incident logs
- regular monitoring of filtering / change control logs
- reporting to relevant Governors / Board / committee / meeting

The Governing Body will ensure that the school's filtering and monitoring arrangements are formally reviewed at least annually. The review will evaluate the effectiveness of filtering and monitoring systems, consider safeguarding risks and emerging technologies, assess whether systems remain appropriate for the age range and needs of pupils, and identify any actions required to strengthen safeguarding arrangements.

**Principal, Heads of School and Senior Leaders**

- The Principal has a duty of care for ensuring the safety (including e-safety) of members of the school community
- The Principal should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.
- The Principal and Head of Children's Services are responsible for ensuring that the E-Safety Coordinator and other relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.
- The Principal will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.

**E-Safety Coordinator**

- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- provides advice for staff
- liaises with school staff team
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments,
- updates the E-Safety Governor to discuss current issues, review incident logs.
- attends relevant meeting / committee of Governors
- reports regularly to Senior Leadership Team. The E-Safety Coordinator will coordinate the school's annual filtering and monitoring review and ensure that appropriate records, recommendations and actions arising from the review are maintained.
- ensures that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- ensures that the school meets required e-safety technical requirements and any Local Authority / other relevant body E-Safety Policy / Guidance that may apply.
- ensures 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, is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant

 © Langley Hall Arts Academy 2022

- that the use of the network, internet, virtual learning environment, remote access systems, email accounts and other school-managed digital services is regularly monitored for both pupils and staff so that misuse, safeguarding concerns or attempted security breaches can be identified, investigated and addressed promptly.

## Teaching and Support Staff

are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the e-safety policy and practices
- they report any suspected misuse or problem to the Designated Safeguarding Lead and E-Safety coordinator for investigation
- all digital communications with students / pupils / parents / carers should be on a professional level and only carried out using official school systems
- E-Safety issues are embedded in all aspects of the curriculum and other activities
- pupils understand and follow the e-safety 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 school 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

The DSL is 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
- cyber-bullying

The Designated Safeguarding Lead will maintain oversight of safeguarding risks arising from the use of technology and will work closely with senior leaders, technical staff and the E-Safety Coordinator to ensure that cyber security risks are appropriately identified, assessed and managed. The Academy recognises that online safety, filtering and monitoring, cyber security incidents, data breaches and emerging technologies may all have safeguarding implications and should therefore be considered within the wider safeguarding framework.

### Pupils

- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations

 © Langley Hall Arts Academy 2022

- 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 cyber-bullying.
- should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy (this document) 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 school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about national / local e-safety campaigns / literature. Parents and carers will be encouraged to support the school in promoting good e-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 the Laser intranet system

## Policy Statement

**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 e-safety is therefore an essential part of the school's e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience.

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

- A planned e-safety curriculum is provided as part of Computing / SMSC other lessons and should be regularly revisited
- Key e-safety messages should be reinforced as part of a planned programme of assemblies and pastoral activities
- Pupils 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.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- 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, 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, pupils 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 thee safety coordinator can temporarily remove

 © Langley Hall Arts Academy 2022

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 e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters, newsletters, website,
- Parents / Carers evenings / sessions
- High profile events / campaigns e.g. Safer Internet Day
- Reference to the relevant web sites / publications

**Education – The Wider Community**

The school will provide opportunities for local community groups / members of the community to gain from the school's e-safety knowledge and experience. This may be offered through the following:

- Providing family learning courses in use of new digital technologies, digital literacy and e-safety
- E-Safety messages targeted towards grandparents and other relatives as well as parents.
- The school / academy website will provide e-safety information for the wider community

**Education & Training – Staff / Volunteers**

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

- A programme of formal e-safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the e-safety training needs of all staff will be carried out regularly.
- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Agreements.
- This E-Safety policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.
- The E-Safety Coordinator will provide advice / guidance / training to individuals as required.

**Training – Governors**

Governors should take part in e-safety training / awareness sessions, with particular importance for those who are members of any / group involved in technology / e-safety / health and safety / child protection. This may be offered in a number of ways:

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

**Cybersecurity and Safeguarding**

 © Langley Hall Arts Academy 2022

Langley Hall Arts Academy recognises that effective cybersecurity is an essential component of safeguarding and pupil welfare. The protection of school systems, personal information, safeguarding records and online services contributes directly to the protection of children and the wider school community.

Cybersecurity risks will be considered as part of the school's safeguarding arrangements and strategic risk management processes. Senior leaders, governors, safeguarding leaders and technical staff will work together to identify emerging cyber risks and ensure that appropriate controls are implemented.

The Academy recognises that cyber incidents may have a significant impact on pupils and staff, including exposure of personal information, interruption of safeguarding systems, loss of educational provision, exposure to harmful content, financial loss or other forms of harm. Cybersecurity will therefore be considered as part of safeguarding decision-making and governance oversight.

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

Langley Hall Arts Academy recognises that filtering and monitoring arrangements form an important part of the school's safeguarding systems and must be reviewed regularly to ensure they remain effective and proportionate.

A formal review of filtering and monitoring arrangements will take place at least annually and additionally where there is a significant safeguarding incident, change in technology, change in the school's systems or identified safeguarding concern.

The annual review will be undertaken by the school's Filtering and Monitoring Review Team, comprising:

- The Principal
- The Designated Safeguarding Lead
- The E-Safety Coordinator
- The school's IT lead or technical support provider
- The E-Safety Governor or nominated safeguarding governor

The review will consider:

- the effectiveness of filtering systems;
- the effectiveness of monitoring systems;
- incidents and trends identified through monitoring reports;
- emerging safeguarding risks;
- the effectiveness of user reporting procedures;
- training needs for staff and pupils;
- any required changes to filtering categories, alerts or monitoring arrangements.

The review will consider activity associated with both pupil and staff accounts and devices where these are connected to, managed by or accessed through school systems. Monitoring arrangements will therefore extend to staff users as well as pupils in order to support safeguarding, information security, professional conduct and the protection of the school community.

Findings, actions and recommendations arising from the review will be documented and reported to senior leaders and governors as appropriate.

As part of this review process, the Academy will undertake an annual cyber-risk assessment. This assessment will consider the security of systems, user behaviour, emerging threats, filtering and monitoring effectiveness, cyber incidents, safeguarding risks, supplier arrangements and business continuity considerations. Findings will be used to inform future safeguarding arrangements, technical controls, staff training and governance oversight.

The Academy will maintain a cyber-awareness programme designed to improve understanding of cyber risks across the school community. The programme will support safe digital behaviours, information security awareness, safeguarding responsibilities and the identification of cyber threats.

All staff will receive cyber-security awareness training at least annually. This training will address current cyber risks, phishing attacks, password security, data protection responsibilities, safeguarding

 © Langley Hall Arts Academy 2022

implications of technology use and incident reporting procedures. At least one governor will also receive appropriate cybersecurity awareness training in order to support governance oversight and challenge.

The e safety coordinator will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities:

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements
- There will be regular reviews and audits of the safety and security of school academy technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school technical systems and devices.
- The Principal 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.
- 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 workstations are protected by up to date virus software.
- An agreed policy is in place for the provision of temporary access of “guests” (e.g. trainee teachers, supply teachers, visitors) onto the school systems.
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

**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 / 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 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 pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- In accordance with guidance from the Information Commissioner’s Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone’s privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other students / pupils in the digital / video images.

 © Langley Hall Arts Academy 2022

- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that students / pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of students / pupils are published on the school website
- Pupil's work can only be published with the permission of the pupil and parents or carers.

**Data Protection**

The Academy recognises that data protection, privacy and cyber security are closely linked. Information arising from filtering systems, monitoring systems, internet usage records, safeguarding systems, email systems and staff or pupil accounts may constitute personal data and will be processed in accordance with data protection requirements.
Individuals with concerns regarding the handling of personal data, monitoring information or browsing data should raise their concerns initially through the school's internal data protection complaints process. The school encourages concerns to be raised in the first instance with the Data Protection Officer so that matters can be investigated and resolved wherever possible before external escalation.
Further information regarding complaints, response timescales, privacy rights and escalation routes is available within the school's Privacy Notices and Complaints and Concerns Policy.

Personal data will be recorded, processed, transferred and made available according to the *Data Protection Act* 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

The school 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 Data Protection Policy (this is the **GDPR Policy SSPo42**)
- It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)
- Responsible persons are appointed / identified - Senior Information Risk Officer (SIRO) and Information Asset Owners (IAOs)
- Risk assessments are carried out

 © Langley Hall Arts Academy 2022

- 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 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.

## 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 school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access).
- Users must immediately report, to the nominated person – in accordance with the school / 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 / pupils or parents / carers (email) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Whole class / group email addresses may be used at KS1, while student pupils at KS2 will be provided with individual school email addresses for educational use.
- Pupils should be taught about e-safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

## Social Media - Protecting Professional Identity

All schools 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 school or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

 © Langley Hall Arts Academy 2022

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

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

School staff should ensure that:

- No reference should be made in social media to pupils, parents / carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

LHAA's use of social media for professional purposes will be checked regularly by the senior risk officer and e-safety committee to ensure compliance with the Social Media, Data Protection, Communications, Digital Image and Video Policies.

**Unsuitable / inappropriate activities**

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The school 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, remarks, proposals or comments that contain or relate to: | 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 pornographic images (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 |

 © Langley Hall Arts Academy 2022

| | | | | | | |
|---|---|---|---|---|---|---|
| | pornography | | | | X | |
| | promotion of any kind of discrimination | | | | X | |
| | threatening behaviour, including promotion of physical violence or mental harm | | | | 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 | |
| Using school systems to run a private business | | | | | X | |
| Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / academy | | | | | X | |
| Infringing copyright | | | | | | X |
| Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords) | | | | | X | |
| Creating or propagating computer viruses or other harmful files | | | | | X | |
| Unfair usage (downloading / uploading large files that hinders others in their use of the internet) | | | | | X | |
| On-line gaming (non-educational) | | | | | X | |
| On-line gambling | | | | | X | |
| On-line shopping / commerce | | | | X | | |
| File sharing | | | | X | | |
| Use of social media for personal use | | | | | X | |
| Use of messaging apps | | | | | X | |
| Use of video broadcasting e.g. YouTube | | | X | | | |

**Filtering and Monitoring of User Activity**

The school's filtering and monitoring systems provide oversight of activity across school-managed networks, devices and services. Monitoring information may relate to both pupil and staff accounts and is used to support safeguarding, cyber security, information governance, professional conduct and compliance with school policies.

The Academy recognises that filtering and monitoring information may contain personal data and will ensure that such information is accessed only by authorised personnel and handled in accordance with data protection requirements, safeguarding procedures and the school's Privacy Notices.

Any concerns identified through monitoring, including safeguarding concerns, cybersecurity concerns, attempted breaches, suspicious activity, misuse of systems or emerging risks, will be reported to the Principal, Designated Safeguarding Lead and other relevant personnel as appropriate and managed through the school's safeguarding and incident management procedures.

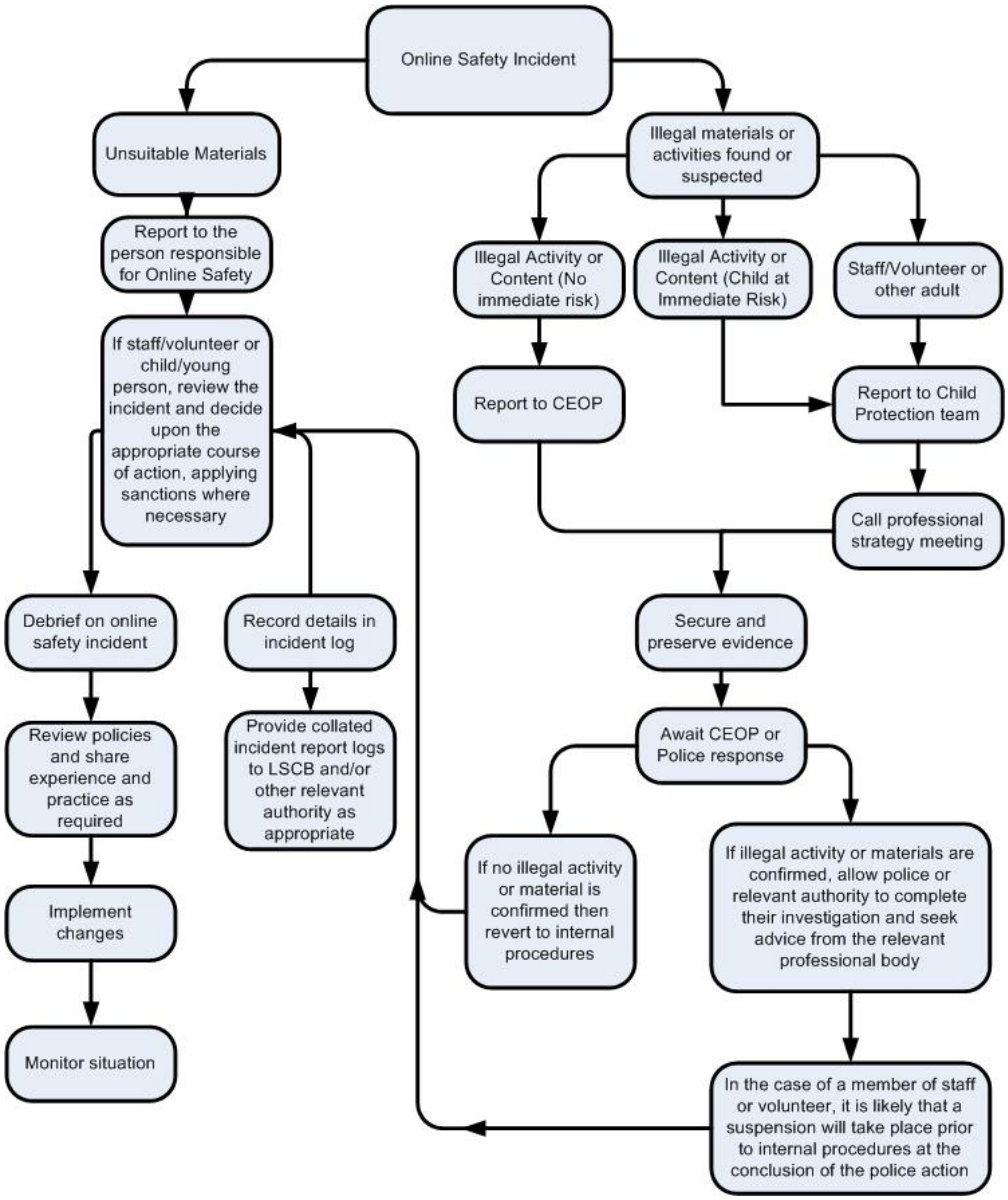
 © Langley Hall Arts Academy 2022

## 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 and appendix) for responding to online safety incidents and report immediately to the police.




 © Langley Hall Arts Academy 2022

**Other Incidents**

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

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

- Have more than one senior member of staff / volunteer 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 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
- other criminal conduct, activity or materials
- **Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.**

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

**School Actions & Sanctions**

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate

 © Langley Hall Arts Academy 2022

manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures as follows:

**Pupils**

| Incidents: | Refer to class teacher | Refer to Headteacher | Refer to Police | Refer to technical support staff for action re filtering / security etc. | Inform parents / carers | Removal of network / internet access rights | Warning | Further sanction |
|---|---|---|---|---|---|---|---|---|
| Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities). | | **X** | **X** | | | | | |
| Unauthorised use of non-educational sites during lessons | X | | | | | | X | |
| Unauthorised use of mobile phone / digital camera / other mobile device | X | X | | | X | | | |
| Unauthorised use of social media / messaging apps / personal email | | | | | X | | X | |
| Unauthorised downloading or uploading of files | X | | | X | | | | |
| Allowing others to access school network by sharing username and passwords | X | | | | | | X | |
| Attempting to access or accessing the school network, using another student's / pupil's account | X | | | | | | X | |
| Attempting to access or accessing the school network, using the account of a member of staff | | X | | | X | | | X |
| Corrupting or destroying the data of other users | | | | X | | | | X |
| Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature | | X | X | | X | | | X |
| Continued infringements of the above, following previous warnings or sanctions | | X | | X | | | | X |
| Actions which could bring the school into disrepute or breach the integrity of the ethos of the school | | X | | X | | | | X |
| Using proxy sites or other means to subvert the school's / academy's filtering system | | | | | X | | X | |
| Accidentally accessing offensive or pornographic | | X | X | X | X | | X | X |

 © Langley Hall Arts Academy 2022

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| material and failing to report the incident | | | | | | | | |
| Deliberately accessing or trying to access offensive or pornographic material | | X | X | | X | | | X |
| Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act | | X | | | | | | X |

**Staff** **Actions / Sanctions**

| Incidents: | Refer to line manager | Refer to Headteacher | Refer to Local Authority / HR | Refer to Police | Refer to Technical Support Staff for action | Warning | Suspension | Disciplinary action |
|---|---|---|---|---|---|---|---|---|
| **Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section or unsuitable / inappropriate activities).** | X | X | | X | | | | X |
| Inappropriate personal use of the internet / social media / personal email | X | X | | | | X | | |
| Unauthorised downloading or uploading of files | X | | | | X | X | | |
| Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account | X | | | | X | X | | |
| Careless use of personal data e.g. holding or transferring data in an insecure manner | X | | | | | X | | |
| Deliberate actions to breach data protection or network security rules | | X | | | X | X | | X |
| Corrupting or destroying the data of other users or causing deliberate damage to hardware or software | | X | | | X | X | | X |
| Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature | | X | X | X | | | X | X |
| Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils | | X | X | | | | | X |
| Actions which could compromise the staff member's professional standing | | X | X | | | | | X |

 © Langley Hall Arts Academy 2022

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Actions which could bring the school into disrepute or breach the integrity of the ethos of the school | | X | | | | | X | |
| Using proxy sites or other means to subvert the school's filtering system | X | | | | | X | X | |
| Accidentally accessing offensive or pornographic material and failing to report the incident | | X | X | | | | | |
| Deliberately accessing or trying to access offensive or pornographic material | | | | X | | | X | |
| Breaching copyright or licensing regulations | | X | | | | | | X |
| Continued infringements of the above, following previous warnings or sanctions | | X | | | | | X | X |

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Surveys / questionnaires of
- students / pupils
- parents / carers
- staff

**Insurance, Governance and Assurance**

The Academy recognises that effective filtering, monitoring and cyber-security arrangements form an important part of its governance framework. Failures in cyber-security controls may expose the school to operational, financial, legal, safeguarding and reputational risks.
The Academy also recognises that cyber insurers increasingly expect organisations to demonstrate effective cyber-security arrangements, including appropriate filtering and monitoring controls, user awareness training and governance oversight. The school will therefore keep cyber-security arrangements under regular review and seek continual improvement in line with recognised good practice and relevant Department for Education standards.

**Monitoring arrangements**
This policy will be reviewed **annually.**

 © Langley Hall Arts Academy 2022