Online Safety Policy

The Bay Learning Trust
The Lodge
Ripley St Thomas
Ashton Road
Lancaster
LA1 4RR

t 01524 581872
e admin@baylearningtrust.com
website baylearningtrust.com

Document Control

This document has been approved for operation within:	**All Trust Establishments**
Date effective from	**March 2025**
Date of next review	**March 2027**
Review period	**24 months**
Status	**Statutory**
Owner	**The Bay Learning Trust**
Version	**v1.0**

Index of content

1. Scope of the Policy

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

The Education and Inspections Act 2006 empowers Executive Headteachers/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 sanctions for inappropriate behaviour. This is pertinent to incidents of cyber-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 electronic devices and the deletion of data. In the case of both acts, action will be taken over issues covered by our Behaviour Policy and Mobile Devices Policy.

We will deal with such incidents within this policy and will, where known, inform parents / carers of incidents of inappropriate Online Safety behaviour that take place out of school.

2. Roles and Responsibilities

The Trust delegates responsibility for on-line safety to the Local Governing Body who may further delegate the day to day responsibility for on-line safety to the Executive Headteacher/Headteacher. The following section outlines the online safety roles and responsibilities of individuals and groups within each academy:

2.1 Governors

The DfE guidance “Keeping Children Safe in Education” states:
“Governing bodies and proprietors should ensure there are appropriate policies and procedures in place in order for appropriate action to be taken in a timely manner to safeguard and promote children’s welfare …. this includes … online safety”

The Directors, as proprietors, are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. Monitoring the effectiveness of this policy will be delegated to the Local Governing Bodies and carried out by those Governors by receiving regular information about online safety incidents and monitoring reports. A member of the Governing Body should take on the role of Safeguarding Governor. The role of the Safeguarding Governor will include online safety. They will monitor online safety by:

- holding regular meetings with the Online Safety Lead
- regularly receiving (collated and anonymised) reports of online safety incidents
- checking that provision outlined in the Online Safety Policy (e.g. online safety education provision and staff training is taking place as intended)

- Ensuring that the filtering and monitoring provision is reviewed and recorded, at least annually, in-line with the DfE Filtering and Monitoring Standards
- Receiving (at least) basic cyber-security training to enable the governors to check that the school meets the DfE Cyber-Security Standards
- reporting to relevant *governors meeting*

The governing body will also support the school in encouraging parents/carers and the wider community to become engaged in online safety activities.

2.2 Executive Headteacher/Headteacher and Senior Leaders

- The Executive Headteacher/Headteacher has a duty of care for ensuring the safety (including online safety) of members of our community, though the day-to-day responsibility for online safety is held by the Designated Safeguarding Lead, as defined in Keeping Children Safe in Education..
- The Executive Headteacher/Headteacher and (at least) another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.
- The Executive Headteacher/Headteacher is responsible for ensuring that the Designated Safeguarding Lead / Online Safety Officer 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 Executive Headteacher/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.
- The Executive Headteacher/Headteacher will receive regular monitoring reports from the Designated Safeguarding Lead / Online Safety Officer.

2.3 Designated Safeguarding Lead (DSL)

The DfE guidance “Keeping Children Safe in Education” states that:

> *“The designated safeguarding lead should take lead responsibility for safeguarding and child protection (including online safety and understanding the filtering and monitoring systems and processes in place). This should be explicit in the role holder’s job description.”*
>
> *They (the DSL) “are able to understand the unique risks associated with online safety and be confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online at school or college”*
>
> *They (the DSL) “can recognise the additional risks that children with special educational needs and disabilities (SEND) face online, for example, from bullying,*

> *grooming and radicalisation and are confident they have the capability to support children with SEND to stay safe online"*

While the responsibility for online safety is held by the DSL and cannot be delegated, the school may choose to appoint an Online Safety Officer or other relevant persons to work in support of the DSL in carrying out these responsibilities. It is recommended that the school reviews the sections below for the DSL and OSL and allocate roles depending on the structure it has chosen

The DSL will:

- hold the lead responsibility for online safety, within their safeguarding role.
- Receive relevant and regularly updated training in online safety to enable them to understand the risks associated with online safety and be confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online
- meet regularly with the online safety governor to discuss current issues, review (anonymised) incidents and filtering and monitoring logs and ensuring that annual (at least) filtering and monitoring checks are carried out
- attend relevant governing body meetings/groups
- report regularly to headteacher/senior leadership team
- be responsible for receiving reports of online safety incidents and handling them, and deciding whether to make a referral by liaising with relevant agencies, ensuring that all incidents are recorded.
- liaise with staff and IT providers on matters of safety and safeguarding and welfare (including online and digital safety)

The school will need to decide whether to appoint an Online Safety Officer to support the DSL. If the DSL & OSO roles are combined the following should be added to the DSL role above.

2.4 Online Safety Officer

The Online Safety Officer will:

- work closely on a day-to-day basis with the Designated Safeguarding Lead (DSL), where these roles are not combined
- promote an awareness of and commitment to online safety education / awareness raising across the school and beyond
- liaise with curriculum leaders to ensure that the online safety curriculum is planned, mapped, embedded and evaluated
- ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place and the need to immediately report those incidents
- provide (or identify sources of) training and advice for staff/governors/parents/carers/learners
- liaise with (school/local authority/MAT/external provider) technical staff, pastoral staff and support staff (as relevant)

- meet regularly with the online safety governor to discuss current issues, review (anonymised) incidents and if possible, filtering and monitoring logs
- ensures that all staff are aware of who to speak to in the event of an online safety incident taking place
- receive reports of online safety issues, being aware of the potential for serious child protection concerns and ensure that these are logged to inform future online safety developments
- receive regularly updated training to allow them to understand how digital technologies are used and are developing (particularly by learners) with regard to the areas defined In Keeping Children Safe in Education:
    - content
    - contact
    - conduct
    - commerce

2.5 Curriculum Leaders

Curriculum and other leaders will work with the DSL/Online Safety Officer to develop a planned and coordinated online safety education programme. This may be provided through:

- PHSE and SRE programmes
- A mapped cross-curricular programme
- assemblies and pastoral programmes
- through relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week.

2.6 Network Manager / Technical Staff

The Network Manager / Technical staff are responsible for ensuring:

- they are aware of and follow the school Online Safety Policy and Technical Security Policy to carry out their work effectively in line with school policy
- 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 as identified by the DfE Meeting Digital and Technology Standards in Schools & Colleges and any Online Safety Policy / Guidance 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
- 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 / Learning Platform / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Executive Headteacher/Headteacher or the Online Safety Officer for investigation.
- the filtering policy is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person
- that monitoring software / systems are implemented and updated.

2.7 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 understand that online safety is a core part of safeguarding
- they have read, understood and signed the **Staff Acceptable Use Agreement**.
- they report any suspected misuse or problem to the Online Safety Officer or other relevant leader for investigation / action, in line with the school safeguarding procedures.
- all digital communications with students / pupils / parents / carers should be on a professional level and only carried out using official school systems.
- online safety issues are embedded in all aspects of the curriculum and other activities.
- 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 school activities (where allowed) and implement our Mobile Devices Policy 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
- where lessons take place using live-streaming or video-conferencing, staff must have full regard to national safeguarding guidance and local safeguarding policies and should take note of the guidance contained in the SWGfL Safe Remote Learning Resource
- have a zero-tolerance approach to incidents of online-bullying, sexual harassment, discrimination, hatred etc
- they model safe, responsible, and professional online behaviours in their own use of technology, including out of school and in their use of social media.

2.8 Students / Pupils

- are responsible for using the academy digital technology systems in accordance with the **Pupil Acceptable Use Agreement** and Online Safety Policy

- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- should 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 our Mobile Devices Policy. They should also know and understand policies on the taking / use of images and on cyber-bullying.
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the academy's Online Safety Policy covers their actions out of school, if related to their membership of the school

2.9 Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The academy will take every opportunity to help parents understand these issues through:

- publishing the school Online Safety Policy on the school website
- providing them with a copy of the learners' acceptable use agreement for signing
- publish information about appropriate use of social media relating to posts concerning the school
- seeking their permissions concerning digital images, cloud services etc
- parents'/carers' evenings, newsletters, website, social media and information about national/local online safety campaigns and literature.

Parents and carers will be encouraged to support the academy in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website and on-line pupil records
- their children's personal devices in the academy (where this is allowed)

3. Reporting and responding

The 2021 Ofsted "Review of Sexual Abuse in Schools and Colleges" highlighted the need for schools to understand that reporting systems do not always respond to the needs of learners. While the report looks specifically at harmful sexual behaviours, schools may wish to address these issues more generally in reviewing their reporting systems. The Ofsted review suggested:

> *"School and college leaders should create a culture where sexual harassment and online sexual abuse are not tolerated, and where they identify issues and intervene early to better protect children and young people. ..In order to do this, they should assume that sexual harassment and online sexual abuse are happening in their setting, even when there are no specific reports, and put in place a whole-school approach to address them. This should include:*

- *routine record-keeping and analysis of sexual harassment and sexual violence, including online, to identify patterns and intervene early to prevent abuse"*

The school will take all reasonable precautions to ensure online safety for all school users but recognises that incidents may occur inside and outside of the school (with impact on the school) which will need intervention. The school will ensure:

- there are clear reporting routes which are understood and followed by all members of the school community which are consistent with the school safeguarding procedures, and with the whistleblowing, complaints and managing allegations policies.
- all members of the school community will be made aware of the need to report online safety issues/incidents
- reports will be dealt with as soon as is practically possible once they are received
- the Designated Safeguarding Lead, Online Safety Lead and other responsible staff have appropriate skills and training to deal with online safety risks.
- if there is any suspicion that the incident involves any illegal activity or the potential for serious harm (see flowchart and user actions chart in the appendix), the incident must be escalated through the agreed school safeguarding procedures, this may include
    - Non-consensual images
    - Self-generated images
    - Terrorism/extremism
    - Hate crime/ Abuse
    - Fraud and extortion
    - Harassment/stalking
    - Child Sexual Abuse Material (CSAM)
    - Child Sexual Exploitation Grooming
    - Extreme Pornography
    - Sale of illegal materials/substances
    - Cyber or hacking offences under the Computer Misuse Act
    - Copyright theft or piracy
- any concern about staff misuse will be reported to the Executive Headteacher/Headteacher, unless the concern involves the Executive Headteacher/Headteacher, in which case the complaint is referred to the CEO of the MAT
- where there is no suspected illegal activity, devices may be checked using the following procedures:
    - one or more senior members of staff should be involved in this process. This is vital to protect individuals if accusations are subsequently reported.
    - conduct the procedure using a designated device that will not be used by learners and, if necessary, can be taken off site by the police should the need arise (should illegal activity be subsequently suspected). Use the same device for the duration of the procedure.
    - 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

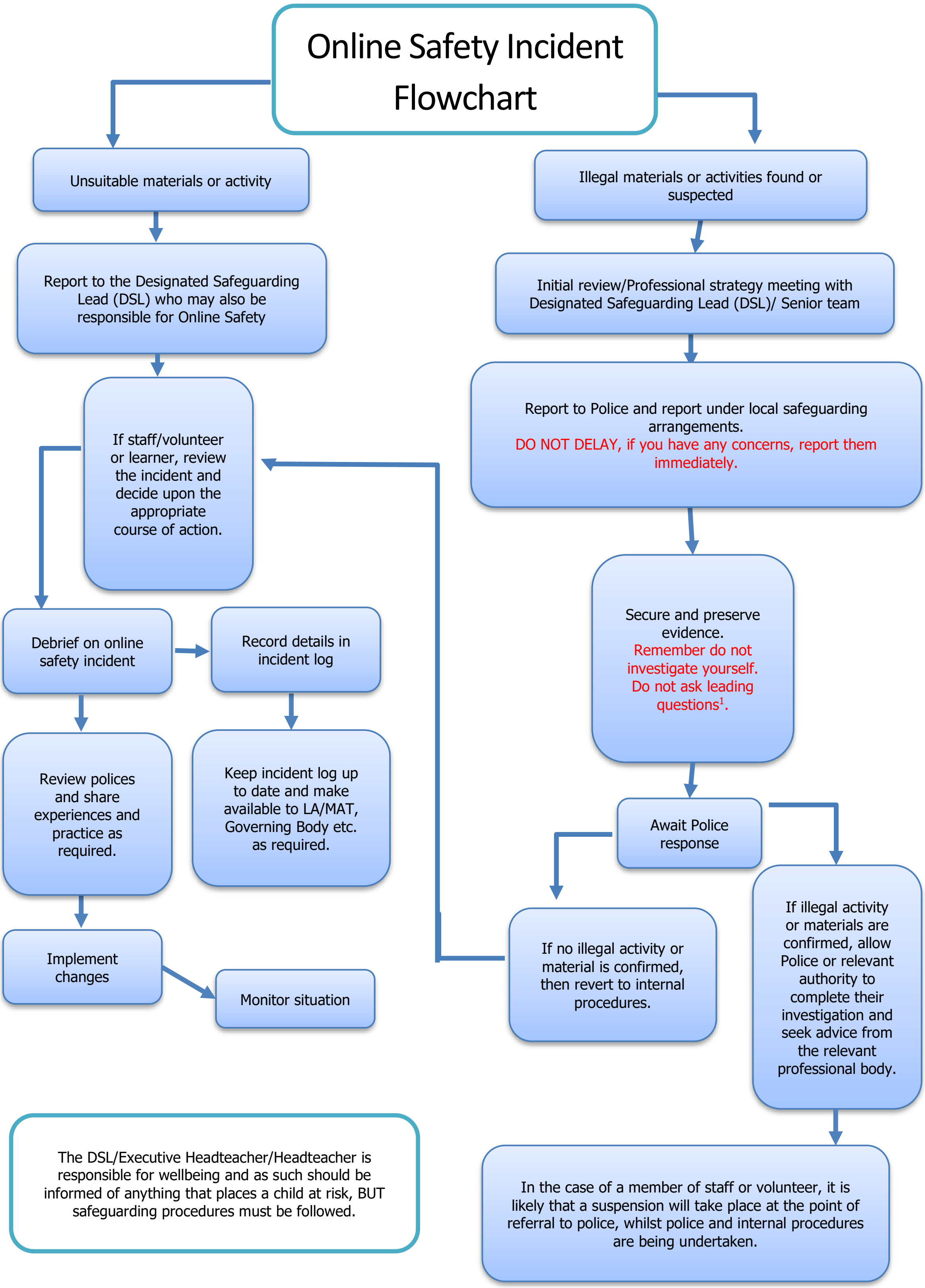
store screenshots of the content on the machine being used for investigation. These may be printed, signed, and attached to the form

  - 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
    - police involvement and/or action
- it is important that those reporting an online safety incident have confidence that the report will be treated seriously and dealt with effectively
- there are support strategies in place e.g., peer support for those reporting or affected by an online safety incident
- incidents should be logged
- relevant staff are aware of external sources of support and guidance in dealing with online safety issues, e.g. local authority; police; Professionals Online Safety Helpline; Reporting Harmful Content; CEOP.
- those involved in the incident will be provided with feedback about the outcome of the investigation and follow up actions (as relevant)
- learning from the incident (or pattern of incidents) will be provided (as relevant and anonymously) to:
  - *staff, through regular briefings*
  - *learners, through assemblies/lessons*
  - *parents/carers, through newsletters, school social media, website*
  - *governors, through regular safeguarding updates*
  - *local authority/external agencies, as relevant (The Ofsted Review into Sexual Abuse in Schools and Colleges suggested "working closely with Local Safeguarding Partnerships in the area where the school or college is located so they are aware of the range of support available to children and young people who are victims or who perpetrate harmful sexual behaviour")*

The school will make the flowchart available to staff to support the decision-making process for dealing with online safety incidents.

School actions

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 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.



Online Safety Incident Flowchart

Unsuitable materials or activity

Report to the Designated Safeguarding Lead (DSL) who may also be responsible for Online Safety

If staff/volunteer or learner, review the incident and decide upon the appropriate course of action.

Debrief on online safety incident

Record details in incident log

Review polices and share experiences and practice as required.

Keep incident log up to date and make available to LA/MAT, Governing Body etc. as required.

Implement changes

Monitor situation

The DSL/Executive Headteacher/Headteacher is responsible for wellbeing and as such should be informed of anything that places a child at risk, BUT safeguarding procedures must be followed.

Illegal materials or activities found or suspected

Initial review/Professional strategy meeting with Designated Safeguarding Lead (DSL)/ Senior team

Report to Police 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 ask leading questions[1].

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.

4. Policy Statements

4.1 Online Safety Education – Students / 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 our academy's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

The 2021 Ofsted "Review of Sexual Abuse in Schools and Colleges" highlighted the need for:

> *"a carefully sequenced RSHE curriculum, based on the Department for Education's (DfE's) statutory guidance, that specifically includes sexual harassment and sexual violence, including online. This should include time for open discussion of topics that children and young people tell us they find particularly difficult, such as consent and the sending of 'nudes'.."*

Keeping Children Safe in Education states:

> "*Governing bodies and proprietors should ensure online safety is a running and interrelated theme whilst devising and implementing their whole school or college approach to safeguarding and related policies and procedures. This will include considering how online safety is reflected as required in all relevant policies and considering online safety whilst planning the curriculum …"*

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

- A planned online safety curriculum should be provided as part of Computing lessons and drop down PSHRE days and should be regularly revisited
- Lessons are matched to need; are age-related and build on prior learning
- Lessons are context-relevant with agreed objectives leading to clear and evidenced outcomes
- Key online safety messages should be reinforced as part of a planned programme of assemblies
- Digital competency is planned and effectively threaded through the appropriate digital pillars in other curriculum areas e.g. PHSE; SRE; Literacy etc. Pupils are taught in all lessons to be critically aware of the materials they access on-line and be guided to validate the accuracy of information.
- it incorporates/makes use of relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week
- the programme will be accessible to learners at different ages and abilities such as those with additional learning needs or those with English as an additional language.

- vulnerability is actively addressed as part of a personalised online safety curriculum e.g., for victims of abuse and SEND.
- Pupils are taught about the risk of online fraud and identity theft
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet. They are also taught about privacy and security
- Pupils are taught about why age restrictions exist and how some sites require a user to verify their age.
- Pupils are taught what the age of digital consent means
- Pupils are taught about the risk of online radicalisation and they 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.
- Programmes of online safety education should incorporate/makes use of relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week
- Students / pupils should be helped to understand the need for the student / pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside 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, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (via the online safety officer) can temporarily remove those sites from the filtered list for the period of study. Once the site is no longer required, staff should inform the Technical Staff (or online safety officer) and the site will be added back into the filtered list.
- More details about the teaching of
    - the underpinning knowledge and behaviours
    - harms and risks

can be found at https://www.gov.uk/government/publications/teaching-online-safety-in-schools/teaching-online-safety-in-schools#underpinning-knowledge-and-behaviours

4.2 Education – Parents / Carers

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring /

regulation of the children’s on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

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

- Letters, newsletters, learning platforms and the website
- regular opportunities for engagement with parents/carers on online safety issues through awareness workshops / parent/carer evenings etc
- high profile events / campaigns e.g. Safer Internet Day

4.3 Education & Training – Staff and volunteers

The DfE guidance “Keeping Children Safe in Education” states:

> “All staff should receive appropriate safeguarding and child protection training (**including online safety**) at induction. The training should be **regularly updated**. In addition, all staff should receive safeguarding and child protection (**including online safety**) updates (for example, via email, e-bulletins, and staff meetings), as required, and at least annually, to continue to provide them with relevant skills and knowledge to safeguard children effectively.”
>
> “Governing bodies and proprietors should ensure... that safeguarding training for staff, **including online safety** training, is integrated, aligned and considered as part of the whole school or college safeguarding approach and wider staff training and curriculum planning.**”**

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 and data protection training will be made available to all staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.
- the training will be an integral part of the school’s annual safeguarding and data protection training for all staff
- all new staff will receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and acceptable use agreements. It includes explicit reference to classroom management, professional conduct, online reputation and the need to model positive online behaviours.
- the Online Safety Officer and Designated Safeguarding Lead (or other nominated person) will receive regular updates through attendance at external training events, (e.g. UKSIC / SWGfL / MAT / LA / other relevant organisations) 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/team meetings/INSET days
- the Designated Safeguarding Lead/Online Safety Officer (or other nominated person) will provide advice/guidance/training to individuals *as required.*

4.4 Training – Governors / Directors

Governors should take part in online safety training sessions, with particular importance for those who are members of any subcommittee involved in technology / online safety / health and safety /safeguarding. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority / National Governors Association / or another relevant organisation.
- Participation in academy training.

A higher level of training will be made available to the Online Safety Governor. This will include:

- Cyber-security training (at least at a basic level)
- Training to allow the governor to understand the school's filtering and monitoring provision, in order that they can participate in the required checks and review.

4.5 Technical – infrastructure / equipment, filtering and monitoring

The school is 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. The school should ensure that all staff are made aware of policies and procedures in place on a regular basis and explain that everyone is responsible for online safety and data protection.

The school has filtering and monitoring systems in place to protect the school, systems and users. The school filtering and monitoring provision is regularly reviewed (at least annually) and updated in response to changes in technology and patterns of online safety incidents/behaviours. Day to day management of filtering and monitoring systems requires the specialist knowledge of both safeguarding and IT staff to be effective. The DSL will have lead responsibility for safeguarding and online safety and the IT network manager and Internet Provider will have technical responsibility.

Filtering

- the school manages access to content across its systems for all users and on all devices using the schools internet provision. The filtering provided meets the standards defined in the DfE Filtering standards for schools and colleges and the guidance provided in the UK Safer Internet Centre Appropriate filtering.
- illegal content (e.g., child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation URL list and the police assessed list of unlawful terrorist content, produced on behalf of the Home Office. Content lists are regularly updated
- there are established and effective routes for users to report inappropriate content, recognising that no system can be 100% effective
- there is a clear process in place to deal with, and log, requests/approvals for filtering changes

- filtering logs are regularly reviewed and alert the Designated Safeguarding Lead to breaches of the filtering policy, which are then acted upon.
- the school has provided enhanced/differentiated user-level filtering (allowing different filtering levels for different abilities/ages/stages and different groups of users: staff/learners, etc.)
- younger learners will use child friendly/age-appropriate search engines e.g. SWGfL Swiggle
- the school has a mobile phone policy and where personal mobile devices have internet access through the school network, content is managed in ways that are consistent with school policy and practice.
- access to content through non-browser services (e.g. apps and other mobile technologies) is managed in ways that are consistent with school policy and practice.

If necessary, the school will seek advice from, and report issues to, the SWGfL Report Harmful Content site.

Monitoring

The school has monitoring systems in place to protect the school, systems and users:

- The school monitors all network use across all its devices and services.
- monitoring reports are urgently picked up, acted on and outcomes are recorded by the Designated Safeguarding Lead, all users are aware that the network (and devices) are monitored.
- There are effective protocols in place to report abuse/misuse. There is a clear process for prioritising response to alerts that require rapid safeguarding intervention.
- Management of serious safeguarding alerts is consistent with safeguarding policy and practice.

The school follows the UK Safer Internet Centre Appropriate Monitoring guidance and protects users and school systems through the use of the appropriate blend of strategies informed by the school's risk assessment. These may include:

- physical monitoring (adult supervision in the classroom)
- internet use is logged, regularly monitored and reviewed
- filtering logs are regularly analysed and breaches are reported to senior leaders
- pro-active alerts inform the school of breaches to the filtering policy, allowing effective intervention.
- where possible, school technical staff regularly monitor and record the activity of users on the school technical systems
- use of a third-party assisted monitoring service to review monitoring logs and report issues to school monitoring lead(s)

Technical Security

The school technical systems will be managed in ways that ensure that the school meets recommended technical requirements:

- responsibility for technical security resides with the Network Manager who may delegate activities to identified roles.
- all users have clearly defined access rights to school technical systems and devices. Details of the access rights available to groups of users will be recorded by the Network Manager and will be reviewed, at least annually, by the Network Manager
- password policy and procedures are implemented. (consistent with guidance from the National Cyber Security Centre)
- the security of their username and password and must not allow other users to access the systems using their log on details.
- all users have responsibility for the security of their username and password and must not allow other users to access the systems using their log on details.
- all school networks and system will be protected by secure passwords. Passwords must not be shared with anyone.
- the administrator passwords for school systems are kept in a secure place, e.g. school safe.
- there is a risk-based approach to the allocation of learner usernames and passwords.
- servers, wireless systems and cabling are securely located and physical access restricted
- appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems and devices 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 endpoint software.
- there are rigorous and verified back-up routines, including the keeping of network-separated (air-gapped) copies off-site or in the cloud,
- The Network Manager is responsible for ensuring that all software purchased by and used by the school is adequately licenced and that the latest software updates (patches) are applied.
- an appropriate system is in place for users to report any actual/potential technical incident/security breach to the relevant person, as agreed)
- use of school devices out of school and by family members is regulated by an acceptable use statement that a user consents to when the device is allocated to them
- personal use of any device on the school network is regulated by acceptable use statements that a user consents to when using the network
- staff members are not permitted to install software on a school-owned devices without the consent of the Network Manager or Headteacher
- removable media is not permitted unless approved by the Headteacher/CFOCOO/CEO
- systems are in place to control and protect personal data and data is encrypted at rest and in transit.
- mobile device security and management procedures are in place (where mobile devices are allowed access to school systems).

- guest users are provided with appropriate access to school systems based on an identified risk profile.

4.6 Mobile Technologies (including BYOD/BYOT)

Mobile technology devices may be school owned/provided or personally owned and might include: smartphone, tablet, notebook / laptop or other technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider internet which may include the school's learning platform and other cloud based services such as email and data storage.

All users should understand that the primary purpose of the use mobile / personal devices in a school context is educational. Teaching about the safe and appropriate use of mobile technologies should be an integral part of the academy's Online Safety education programme.

4.7 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 students / 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 strategies to reduce the likelihood of the potential for harm:

- the school may use live-streaming or video-conferencing services in line with national and local safeguarding guidance / policies
- When using digital images, staff should inform and educate students / 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.
- Permission from parents or carers will be obtained before photographs of students / pupils are published on the school website / social media / local press
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at academy events for their own personal use (as such use 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.

- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow academy policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school / academy equipment, the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school / academy into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs, except in the media in accordance with consent given as part of Data Protection Act 2018/GDPR.
- photographs published on the website, or elsewhere that include learners will be selected carefully and will comply with Online Safety Policy
- written permission from parents or carers will be obtained before photographs of learners are taken for use in school or published on the school website/social media. (see parents and carers acceptable use agreement in the Appendix). Permission is not required for images taken solely for internal purposes
- images will be securely stored in line with the school retention policy

4.8 Online publishing

The school communicates with parents/carers and the wider community and promotes the school through:

- Public-facing website
- Social media
- Online newsletters
- Learning Platforms, such as School Synergy

The school ensures that online safety policy has been followed in the use of online publishing e.g., use of digital and video images, copyright, identification of young people, publication of school calendars and personal information – ensuring that there is least risk to members of the school community, through such publications.

Where learner work, images or videos are published, their identities are protected, and full names are not published.

5. Data Protection

For more information, please refer to the Data Protection Policy.

6. Communications

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.
- Users must immediately report, to the Executive Headteacher/Headteacher, Online Safety Officer or Data Protection Officer – in accordance with the academy policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and students / 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 (monitored) academy systems. Personal email addresses, text messaging or social media must not be used for these communications.
- 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.
- Personal information should not be posted on the school / academy website and only official email addresses should be used to identify members of staff.

6.1 Social Media - Protecting Professional Identity

Below is a summary of key information regarding Social Media. Please refer to the Trust Social Media Policy for more information.

All schools, academies and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools/academies and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the academy 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
- Education/training being provided including acceptable use, age restrictions, social media risks, digital and video images policy, checking of settings, data protection and reporting issues. Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk
- guidance for learners, parents/carers

Academy staff should ensure that:

- No reference should be made in social media to students / pupils, parents / carers or school / academy staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the academy
- 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 the online safety officer
- Clear processes for the administration and monitoring of these accounts – involving the online safety officer and the DPO
- A code of behaviour for users of the accounts which is discussed with the Online Safety Officer before accounts are made available
- Systems for reporting and dealing with abuse and misuse
- Understanding of how incidents may be dealt with under school / academy disciplinary procedures

Personal Use:

- Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with the academy or impacts on the academy, it must be made clear that the member of staff is not communicating on behalf of the academy with an appropriate disclaimer. Such personal communications are within the scope of this policy
- Personal communications which do not refer to or impact upon the school are outside the scope of this policy
- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken

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

- when parents/carers express concerns about the school on social media we will urge them to make direct contact with the school, in private, to resolve the matter. Where this cannot be resolved, parents/carers should be informed of the school complaints procedure.

The academy's use of social media for professional purposes will be checked regularly by the Online Safety Officer to ensure compliance with the school policies. In the event of any social media issues that the school is unable to resolve support may be sought from the Professionals Online Safety Helpline.

6.2 On line teaching and video conferencing with pupils

The following is taken directly from "Guidance for Safer Working Practice for those working with Children and Young People in Educational Settings" (Addendum April 2020)" produced in response to online teaching needed during the COVID-19 crisis.

Staff should always maintain appropriate professional boundaries, avoid behaviour which could be misinterpreted by others and report any such incident to a senior manager. This is as relevant in the online world as it is in the classroom; staff engaging with pupils and / or parents online have a responsibility to model safe practice at all times.

Staff should ensure they are dressed decently, safely and appropriately for the tasks they undertake; this also applies to online or virtual teaching or when working with small groups on site (in the case of schools who remain open to vulnerable children or those of critical workers)

Staff engaging in online learning should display the same standards of dress and conduct that they would in the real world; they should also role model this to pupils and parents. The following points should be considered:-

- think about the background; photos, artwork, identifying features, mirrors – ideally the backing should be blurred
- staff and pupils should be in living / communal areas – no bedrooms
- staff and pupils should be fully and appropriately dressed
- filters at a child's home may be set at a threshold which is different to the school
- resources / videos must be age appropriate – the child may not have support immediately to hand at home if they feel distressed or anxious about content

It is the responsibility of the staff member to act as a moderator; raise any issues of suitability (of dress, setting, behaviour) with the child and / or parent immediately and end the online interaction if necessary. Pupils should mute their microphones when the teacher is speaking. Some pupils may wish to turn off or cover their camera to make them feel more comfortable – this is perfectly acceptable. Pupils may ask a parent to be with them to help them – again, this is perfectly acceptable. As in any lesson, do not accept poor behaviour or any inappropriate language; pupils should stay within normal lesson expectations. Pupils who do not adhere to this should be removed from the video conference and the matter taken up with a line manager.

Video conferencing lessons with pupils should be recorded for safeguarding purposes. However, it is important that data protection concerns are taken into consideration. The Trust has notified parents and pupils that such lessons will be recorded in the Acceptable Use Policy, but staff should remind participants **at the beginning of each lesson** that it will be recorded for the purpose of safeguarding.

If a staff member believes that a child or parent is recording the interaction, the lesson should be brought to an end or that child should be logged out immediately. Staff and pupil "Acceptable Use Policies" clearly state the standards of conduct required.

Appendix 1 - Table of user actions

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not access online content (including apps, games, sites) to make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	**Any illegal activity for example:** • Child sexual abuse imagery* • Child sexual abuse/exploitation/grooming • Terrorism • Encouraging or assisting suicide • Offences relating to sexual images i.e., revenge and extreme pornography • Incitement to and threats of violence • Hate crime • Public order offences - harassment and stalking • Drug-related offences • Weapons / firearms offences • Fraud and financial crime including money laundering					**X**
Users shall not undertake activities that might be classed as cyber-crime under the Computer Misuse Act (1990)	• Using another individual's username or ID and password to access data, a program, or parts of a system that the user is not authorised to access (even if the initial access is authorised) • Gaining unauthorised access to school networks, data and files, through the use of computers/devices • Creating or propagating computer viruses or other harmful files • Revealing or publicising confidential or proprietary information (e.g., financial / personal information, databases, computer / network access codes and passwords) • Disable/Impair/Disrupt network functionality through the use of computers/devices • Using penetration testing equipment (without relevant permission)					**X**
Users shall not undertake activities that are not illegal but are classed as unacceptable in school policies:	Accessing inappropriate material/activities online in a school setting including pornography, gambling, drugs. (Informed by the school's filtering practices and/or AUAs)			X	X	
	Social media				X	
	Online gambling				X	
	Taking photos on mobile phones/cameras				X	
	Online gaming				X	
	Promotion of any kind of discrimination				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				X	
	Infringing copyright				X	
	Unfair usage (downloading/uploading large files that hinders others in their use of the internet)			X	X	

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
	Any other information which may be offensive to others or breaches the integrity of the ethos of the school or brings the school into disrepute				X	