L.E.A.D. Academy Trust
Lead • Empower • Achieve • Drive

L.E.A.D. ACADEMY TRUST

Online Safety Policy

Policy/Procedure management log

Document name	Online Safety Policy
Date approved	Trust approval January 2025
Date issued	**November 2025**
Date of review	**November 2026**

Introduction – L.E.A.D Academy Trust

L.E.A.D. Academy Trust fully recognises its moral and statutory responsibility to safeguard and promote the welfare of all pupils. The Trust endeavours to provide a safe and welcoming environment in all its academies, where children are respected and valued.

Section 157 of the Education Act 2002 and the Education (Independent Schools Standards) (England) Regulations 2003 require proprietors of independent schools (including academies and city technology colleges) to have arrangements to safeguard and promote the welfare of children.

Aims

- To ensure that all practices of each Academy and its stakeholders contribute towards the safeguarding and promoting of the welfare of all young people – pupils' welfare is of paramount importance.
- To emphasise how online safety is part of safeguarding and promoting the welfare of all young people and is the primary responsibility of all staff, governors, and volunteers.
- To outline the safe working practices that all staff, governors, and volunteers should undertake when working with young people.
- To communicate clear procedures for identifying, reporting, and recording suspected cases of abuse, extremism, and radicalisation.
- To support the mission, vision and values of the Trust and its member academies.

Who is responsible for the policy?

- The Trust has overall responsibility for the development and effective operation of this policy. The Trust has delegated day-to-day responsibility for operating the policy to each individual Trust Academy, the Academy governing body (AGB) and the Headteacher.
- The AGB and senior leadership team at each Trust Academy have specific responsibilities to ensure the fair application of this policy and all are responsible for supporting colleagues and ensuring its success.
- This policy must be implemented alongside the procedural guidance set out by the local authority in which the Academy is located.

The Trust's commitment

- Everyone who comes into contact with children and their families has a role to play in safeguarding children. Academy staff are particularly important as they are in a position to identify concerns early and provide help for children, and to prevent concerns from escalating.
- The Trust is committed to providing safe, caring, and welcoming environments where every child is able to reach their full potential free from harm, abuse, and discrimination. All staff and volunteers are expected to discharge their safeguarding responsibilities, including online safety, effectively and

recognise that high self-esteem, confidence, peer support and clear lines of communication with trusted adults help all children, especially those at risk of or suffering abuse, to thrive.

- All academies will be alert to the signs of abuse, neglect and radicalisation and follow procedures to ensure that children receive effective support, protection, and justice.
- Academies will work with social care, the police, health services and other services (such as Channel co-ordinators/police practitioners where appropriate) to promote the welfare of children and protect them from harm.

Online Safety Policy - scope

This Online Safety Policy outlines the commitment of Witham St Hughs Academy to safeguard members of our Academy community online in accordance with statutory guidance and best practice.

This Online Safety Policy applies to all members of the Academy community (including staff, learners, governors, volunteers, parents and carers, visitors, community users) who have access to and are users of Academy digital systems, both in and out of our Academy. It also applies to the use of personal digital technology on the Academy site (where allowed).

Witham St Hughs Academy will deal with such incidents within this policy and associated behaviour, safeguarding and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that take place out of our Academy.

Policy development, monitoring and review

This Online Safety Policy has been developed by the

- Headteacher/senior leaders
- Designated safeguarding lead (DSL)
- Staff – including teachers/support staff/technical staff
- Governors
- Parents and carers
- Community users

Consultation with the whole Academy community has taken place through a range of formal and informal meetings.

Schedule for development, monitoring and review

This Online Safety Policy was approved by the *Academy* governing *body on:*	November 2025
The implementation of this Online Safety Policy will be monitored by:	Emily Broadley, Michelle Dexter, Hannah Younger.
Monitoring will take place at regular intervals:	November 2026
The *governing body* will receive a report on the implementation of the Online Safety Policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals:	November 2026
The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new technological developments, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	November 2026
Should serious online safety incidents take place, the following external persons/agencies should be informed:	Helen Tunney (Director of Schools), Becky Hyder (safeguarding lead) and police as appropriate.

Process for monitoring the impact of the Online Safety Policy

The Academy will monitor the impact of the policy using:

- Logs of reported incidents
- Filtering and monitoring logs
- Internal monitoring data for network activity
- Surveys/questionnaires of:
    - learners
    - parents and carers
    - staff.

Policy and leadership

Responsibilities

To ensure the online safeguarding of our Academy community it is important that all members work together to develop safe and responsible online behaviours, learning from each other and from good practice elsewhere, reporting inappropriate online behaviours, concerns, and misuse as soon as these become

apparent. While this will be a team effort, the following sections outline the online safety roles and responsibilities of individuals and groups within the Academy.

Headteacher and senior leaders

- The headteacher has a duty of care for ensuring the safety (including online safety) of members of our Academy and fostering a culture of safeguarding. 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 headteacher and (at least) another member of the senior leadership team will be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.
- The headteacher/senior leaders are responsible for ensuring that the Designated Safeguarding Lead, L.E.A.D I.T. Services and their technical staff and other relevant staff carry out their responsibilities effectively and receive suitable training to enable them to carry out their roles and train other colleagues, as relevant.
- The headteacher/senior leaders will ensure that there is a system in place to allow for monitoring and support of those in the Academy who carry out the internal online safety monitoring role.
- The headteacher/senior leaders will receive regular monitoring reports from the Designated Safeguarding Lead.
- The headteacher/senior leaders will work with the responsible Governor, the designated safeguarding lead (DSL) and L.E.A.D I.T. Services in all aspects of filtering and monitoring.

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".*
>
> *"Governing bodies and proprietors should ensure an appropriate senior member of staff, from the Academy or college leadership team, is appointed to the role of designated safeguarding lead. 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)"*

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy e.g. by asking the questions posed in the UKCIS document "Online Safety in Schools and Colleges – questions from the Governing Body".

This review will be carried out by the governing body whose members will receive regular information about online safety incidents and monitoring reports. A member of the governing body will take on the role of Online Safety Governor to include:

- Regular meetings with the Designated Safeguarding 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. (The review will be conducted by members of the SLT, the DSL, and L.E.A.D. I.T Services and involve the responsible governor) - in-line with the *DfE Filtering and Monitoring Standards*
- Reporting to relevant governors meeting
- Receiving (at least) basic cyber-security training to enable the governors to check that the Academy meets the *DfE Cyber-Security Standards*

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

Designated Safety Lead (DSL)

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 Academy 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 Academy may choose to appoint an Online Safety Lead or other relevant persons to work in support of the DSL in carrying out these responsibilities.

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, 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)

Curriculum leads

Curriculum leads will work with the DSL to develop a planned and coordinated online safety education programme.

This will be provided through:

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

Teaching and support staff

Academy staff are responsible for ensuring that:

- They have an awareness of current online safety matters/trends and of the current 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 (AUA)
- They immediately report any suspected misuse or problem to DSL for investigation/action, in line with the Academy safeguarding procedures
- All digital communications with learners and parents/carers are on a professional level and only carried out using official Academy systems. In line with the staff Code of Conduct and Acceptable Use Agreements
- Online safety issues are embedded in all aspects of the curriculum and other activities
- Ensure learners understand and follow the Online Safety Policy and acceptable user agreements. Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- They supervise and monitor the use of digital technologies, which include mobile devices, cameras, etc., in lessons and other activities (where allowed) and implement current policies regarding these devices
- In lessons where internet use is pre-planned learners are guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
- Where lessons take place using live-streaming or video-conferencing, there is regard to national safeguarding guidance and local safeguarding policies (e.g the guidance contained in the SWGfL Safe Remote Learning Resource)
- There is 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 the Academy and in their use of social media.

L.E.A.D I.T. Services

The DfE Filtering and Monitoring Standards says:

"Senior leaders should work closely with governors or proprietors, the designated safeguarding lead (DSL) and IT service providers in all aspects of filtering and monitoring. Your IT service provider may be a staff technician or an external service provider."

"Day to day management of filtering and monitoring systems requires the specialist knowledge of both safeguarding and IT staff to be effective. The DSL should work closely together with IT service providers to meet the needs of your setting. You may need to ask filtering or monitoring providers for system specific training and support."

"L.E.A.D. I.T. Services have technical responsibility for:

- Maintaining filtering and monitoring systems
- Providing filtering and monitoring reports
- Completing actions following concerns or checks to systems"

"L.E.A.D. I.T. Services will work with the senior leadership team and DSL to:

- Procure systems
- Identify risk
- Carry out reviews
- Carry out checks"

As we at Witham St Hughs Academy have a technology service provided by L.E.A.D. I.T. Services, it is our responsibility to ensure that L.E.A.D. I.T. Services carries out all the online safety measures that the Academy's obligations and responsibilities require. It is also important that L.E.A.D. I.T. Services follows and implements our Online Safety Policy and procedures.

L.E.A.D. I.T. Services is responsible for ensuring that:

- They are aware of and follow our Online Safety Policy and Technical Security Statement to carry out their work effectively
- Our Academy technical infrastructure is secure and is not open to misuse or malicious attack
- We meet (as a minimum) the required online safety technical requirements as identified by the '*DfE Meeting Digital and Technology Standards in Schools & Colleges'* and guidance from local authority / the Trust or other relevant body
- There is clear, safe, and managed control of user access to networks and devices
- 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
- The use of technology is regularly and effectively monitored in order that any misuse/attempted misuse can be reported to Trust Director of IT for investigation and action
- The filtering statement is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person (see appendix 'Technical Security statement' for good practice).
- Monitoring systems are implemented and regularly updated as agreed in our Academy policies

Learners

- Are responsible for using the Academy digital technology systems in accordance with our learner acceptable use agreements and Online Safety Policy
- Should understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- Should know what to do if they or someone they know feels vulnerable when using online technology.
- Should understand the importance of adopting good online safety practice when using digital technologies out of the Academy and realise that the Academy 's Online Safety Policy covers their actions out of the Academy, if related to their membership of the Academy.

Parents and carers

Parents and carers play a crucial role in ensuring that their children understand the need to use the online services and devices in an appropriate way.

At Witham St Hughs Academy we will take every opportunity to help parents and carers understand these issues through:

- publishing the Academy Online Safety Policy on our website
- providing them with a copy of the learners' acceptable use agreement
- publish information about appropriate use of social media relating to posts concerning the Academy.
- seeking their permissions concerning digital images, cloud services etc (see parent/carer AUA in the appendix)
- 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:

- reinforcing the online safety messages provided to learners.
- the safe and responsible use of their children's personal devices.

Community users

Community users who access the Academy Internet as part of the wider Academy provision will be expected to agree to the AUG, via a link to the Academy website.

Policy

Online Safety Policy

Witham St Hughs Academy Online Safety Policy:

- sets expectations for the safe and responsible use of digital technologies for learning, administration, and communication

- allocates responsibilities for the delivery of the policy
- is regularly reviewed in a collaborative manner, taking account of online safety incidents and changes/trends in technology and related behaviours
- establishes guidance for staff in how they should use digital technologies responsibly, protecting themselves and the Academy, and how they should use this understanding to help safeguard learners in the digital world
- describes how we will help prepare learners to be safe and responsible users of online technologies
- establishes clear procedures to identify, report, respond to and record the misuse of digital technologies and online safety incidents, including external support mechanisms
- is supplemented by a series of related acceptable use agreements
- is made available to staff at induction and through normal communication channels
- is published on our Academy website.

Acceptable use

Acceptable use agreements

Our acceptable use agreement is a document that outlines Witham St Hughs Academy expectations on the responsible use of technology by its users. It is signed or acknowledged by staff as part of their conditions of employment. We also require learners and parents/carers to sign it, though it is more important for these to be regularly promoted, understood and followed rather than just signed. There is a range of acceptable use agreements in the appendices along with a table of actions.

Witham St Hughs Academy Online Safety Policy and acceptable use agreements define acceptable use. The acceptable use agreements will be communicated/re-enforced through:

- learner handbook
- staff induction and handbook
- splash screens
- digital signage
- posters/notices around where technology is used
- communication with parents/carers
- building it into education sessions
- Academy website
- peer support.

When using communication technologies, we at Witham St Hughs Academy considers the following as good practice:

- when communicating in a professional capacity, staff will ensure that the technologies they use are officially sanctioned by the Academy.
- any digital communication between staff and learners or parents/carers (e-mail, Academy social media, learning platform, etc.) must be professional in tone and content. Personal e-mail addresses, text messaging or social media must not be used for these communications.
- Staff are expected to follow good practice when using personal social media regarding their own professional reputation and that of the Academy and its community

- users should immediately report to a nominated person – in accordance with 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.
- relevant policies and permissions should be followed when posting information online e.g., Academy website and social media. Only Academy e-mail addresses should be used to identify members of staff and learners.

Reporting and responding to sexual harassment and abuse

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. The Ofsted review suggested:

> *"Academy 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-Academy 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"*

Therefore, we at Witham St Hughs Academy will take all reasonable precautions to ensure online safety for all users but recognise that incidents may occur inside and outside of our Academy (with impact on the Academy) which will need intervention. We will ensure:

- there are clear reporting routes which are understood and followed by all members of the Academy community which are consistent with our safeguarding procedures, and with the whistleblowing, complaints and managing allegations policies. At Witham St Hughs Academy we use Confide.
- all members of our 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 during Academy hours (within 24 hours of receiving)
- the Designated Safeguarding 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 will be escalated through the agreed Academy 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
  - AI generated inappropriate imagery

- any concern about staff misuse will be reported to the Headteacher, unless the concern involves the Headteacher or where there is a conflict of interest in reporting to the Headteacher, in which case the complaint is referred to the Director of Schools, Trust DSL and the local authority.
- where there is no suspected illegal activity, devices may be checked as follows:
  - contact made to a senior member of the L.E.A.D. IT Services team to provide logs for devices and individuals and support the review of logs as a part of the investigation team.
  - two senior members of staff must be present. This is vital to protect individuals if accusations are subsequently reported.
  - use an Academy owned 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 a search of the users' 'history', but also that the sites and content visited are and recorded. Links to websites which are suspected of showing child sexual abuse should not be opened or investigated. If unsure, a site should not be viewed.
  - 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 Headteacher 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 / Trust (as relevant)
    - 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 on MyConcern and where appropriate Confide
- 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 / necessary)
- 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, Academy social media, website
  - governors, through regular safeguarding updates
  - local authority/external agencies, as relevant

Where illegal activity is suspected the Academy will:

- Contact the LADO
- Contact the Police
- Confiscate devices owned by the Academy i.e. laptop/phone

> *The Ofsted Review into Sexual Abuse in Schools and Colleges suggested "working closely with Local Safeguarding Partnerships in the area where the Academy 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 Academy will make the flowchart below available to staff to support the decision-making process for dealing with online safety incidents.

Harmful Sexual Behaviour (HSB)

At Witham St Hughs Academy we recognise that sexual violence and sexual harassment occurring online (either in isolation or in connection with face-to-face incidents) can introduce a number of complex factors. Amongst other things, this can include widespread abuse or harm across social media platforms that leads to repeat victimisation. Online concerns can be especially complicated, and support is available from a range of organisations – see the links section. For this reason, we ensure that we have a robust, up-to-date and comprehensive online safety policy which links to other relevant safeguarding policies.

Our Academy has a zero-tolerance approach to any harmful sexual behaviour involving children and acknowledges that it could be occurring at Witham St Hughs Academy and in our community. We adopt a proactive approach to assessing prevalence, responding to incidents and challenging and changing behaviour. This statement applies to all governors, staff and learners.

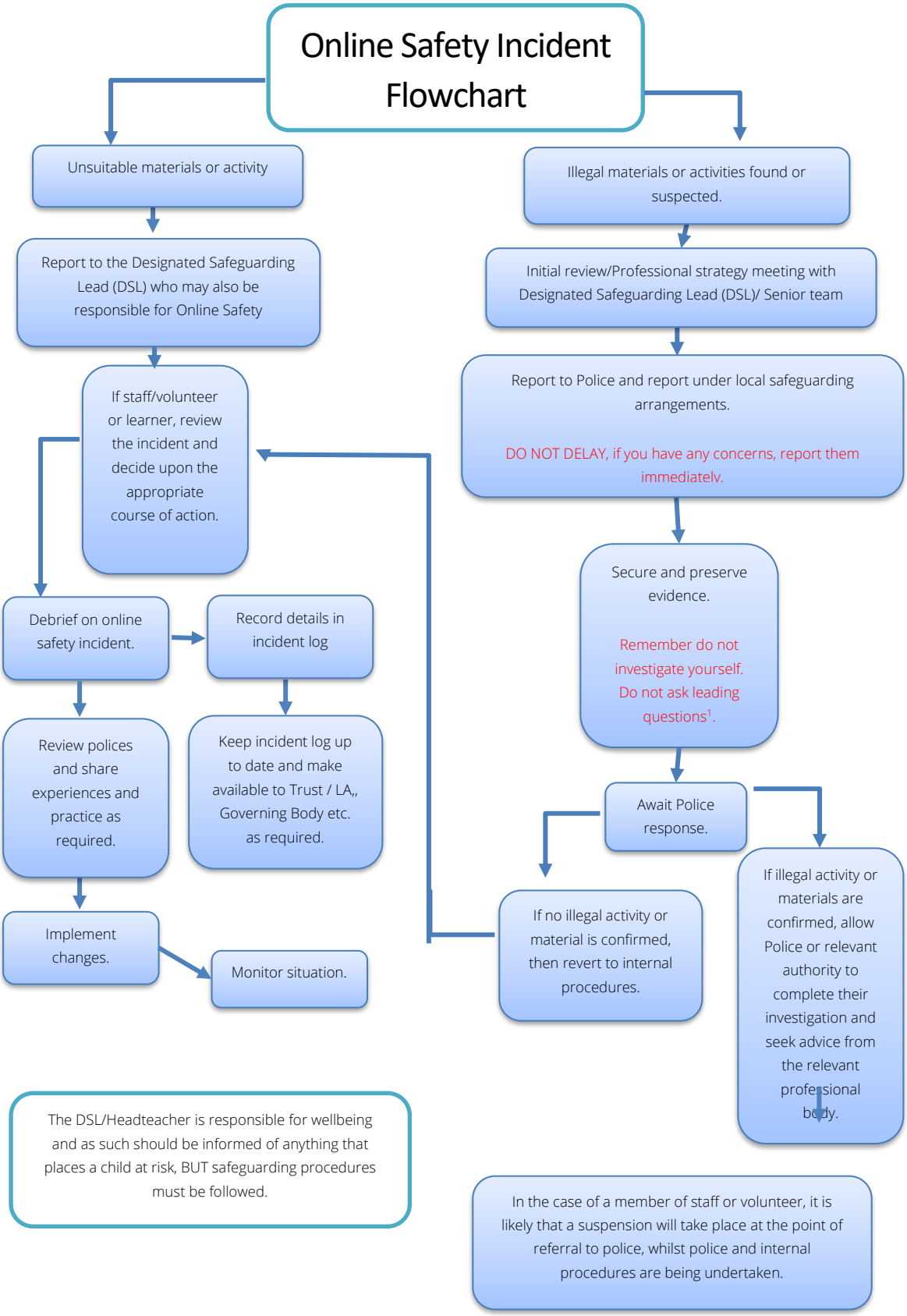
We have a statutory duty to safeguard the children in our setting. We work together to foster an environment that creates healthy relationships for children and young people.

Our whole-Academy approach encourages healthy relationships and works to prevent harmful sexual behaviour. We provide high quality education within the curriculum to reduce the likelihood of the situations occurring.

We recognise that HSB is harmful to both the child/children affected by the behaviours and the child/children who displayed the behaviour and provide ongoing support for all involved.

Our approach is to treat each incident of sexual behaviour as a safeguarding incident in the first instance - we then distinguish between behaviours that are exploratory and part of healthy age and ability appropriate development and those that may be harmful.

As an Academy we provide regular opportunities for staff to understand what harmful sexual behaviours might look like and what they should do in the event of a report.


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 Trust / LA,, Governing Body etc. as required.
Implement changes.
Monitor situation.
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 immediatelv.
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.
The DSL/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.
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.

Academy actions

It is more likely that we at Witham St Hughs Academy will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of our community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary/safeguarding procedures.

Responding to learner actions

Incidents	Refer to class teacher/tutor	Refer to Head of Department / Principal Teacher / Deputy Head	Refer to Headteacher	Refer to Police/Social Work	Refer to L.E.A.D. I.T Services / local authority technical support for advice/action	Inform parents/carers	Remove device/ network/internet access rights	Issue a warning	Further sanction, in line with behaviour policy
Deliberately accessing or trying to access material that could be considered illegal (see list on unsuitable/inappropriate activities in appendices).		X	X	X	X	X	X		X
Attempting to access or accessing the Academy network, using another user's account (staff or learner) or allowing others to access Academy network by sharing username and passwords	X	X			X			X	X
Corrupting or destroying the data of other users.	X	X			X				X
Sending an e-mail, text or message that is regarded as offensive, harassment or of a bullying nature	X	X	X			X			X
Unauthorised downloading or uploading of files or use of file sharing.	X	X			X			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		X	X	X		X

Incidents	Refer to class teacher/tutor	Refer to Head of Department / Principal Teacher / Deputy Head	Refer to Headteacher	Refer to Police/Social Work	Refer to L.E.A.D. I.T Services / local authority technical support for advice/action	Inform parents/carers	Remove device/ network/internet access rights	Issue a warning	Further sanction, in line with behaviour policy
Deliberately accessing or trying to access offensive or pornographic material.		X	X	X	X	X	X		X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act.		X			X				X
Unauthorised use of digital devices (including taking images)		X	X		X	X	X		X
Unauthorised use of online services	X	X			X				X
Actions which could bring the Academy into disrepute or breach the integrity or the ethos of the school.	X	X	X		X	X		X	X
Continued infringements of the above, following previous warnings or sanctions.			X		X	X			X

Searching, screening and confiscating

Members of staff will be made aware of the Academy ’s statement on "Electronic devices – searching, confiscation and deletion”, held within the Academy Behaviour Policy:

- at induction
- at regular updating sessions on the Academy ’s online safety / safeguarding / behaviour management policy
- in safeguarding training and briefings

Members of staff authorised by the Headteacher to carry out searches for and of electronic devices and to access and delete data/files from those devices should receive training that is specific and relevant to this role.

Specific training is required for those staff who may need to judge whether material that is accessed is inappropriate or illegal.

The Headteacher will publicise the Academy behaviour policy, in writing, to staff, parents/carers and learners at least once a year.

Responding to staff actions

Incidents	Refer to line manager	Refer to Headteacher/ Principal	Refer to local authority/MAT/HR	Refer to Police	Refer to LA / Technical Support Staff for action re filtering, etc.	Issue a warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list on Page 12 in earlier section on unsuitable / inappropriate activities)		X	X	X	X	X	X	X
Deliberate actions to breach data protection or network security rules.		X	X		X			X
Deliberately accessing or trying to access offensive or pornographic material		X	X	X Police informed if content illegal.	X		X	X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		X	X	Depends on data	X		X	X
Using proxy sites or other means to subvert the school's filtering system.		X	X	Depends on data		X	Depends on data	X
Unauthorised downloading or uploading of files or file sharing		X	X	Depends on data		X	Depends on data	X
Breaching copyright or licensing regulations.		X	X			X		
Allowing others to access Academy network by sharing username and passwords or	X	X	LEAD I.T. Services		X	X	X	If repeatedly

Incidents	Refer to line manager	Refer to Headteacher/ Principal	Refer to local authority/MAT/HR	Refer to Police	Refer to LA / Technical Support Staff for action re filtering, etc.	Issue a warning	Suspension	Disciplinary action
attempting to access or accessing the Academy network, using another person's account.								happens and impact
Sending an e-mail, text or message that is regarded as offensive, harassment or of a bullying nature	X	X	Depending on nature	Depending on nature	X	X	Possible	Possible
Using personal e-mail/social networking/messaging to carry out digital communications with learners and parents/carers	X							X
Inappropriate personal use of the digital technologies e.g. social media / personal e-mail	X							X
Careless use of personal data, e.g. displaying, holding or transferring data in an insecure manner	X		X		X			X
Actions which could compromise the staff member's professional standing		X	X		X			X
Actions which could bring the Academy into disrepute or breach the integrity or the ethos of the school.		X	X		X			X
Failing to report incidents whether caused by deliberate or accidental actions		X	X	Depending on nature	X	Depending on nature		X
Continued infringements of the above, following previous warnings or sanctions.		X	X		X		Depending on nature	X

Online safety education programme

While regulation and technical solutions are particularly important, their use must be balanced by educating learners to take a responsible approach. The education of learners in online safety is therefore an essential part of Witham St Hughs Academy online safety provision. Learners need the help and support of our Academy to recognise and avoid online safety risks and develop 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 Academy 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 will be a focus in all areas of the curriculum and staff will reinforce online safety messages. Our broad curriculum gives pupils opportunities to experience life in all its diversity, to acquire knowledge, understanding, and skills that significantly impact personal development, behaviour, and welfare, and equips every child with the knowledge and skills required for personal safeguarding.

Our PSE curriculum covers all areas of Safeguarding through each of the strands to a different degree; however, some go into more detail. We are sensitive in our teaching and recognise that some more sensitive subjects need to be taught at an age-appropriate level, or at a small group or 1:1 level where a more urgent need arises.

- A planned online safety curriculum for all year groups matched against a nationally agreed framework- National Centre for Computing Education
- 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
- Learner need and progress are addressed through effective planning and assessment
- Digital competency is planned and effectively threaded through the appropriate digital pillars in other curriculum areas e.g. PHSE; SRE; Literacy etc
- Incorporating/making use of relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week
- The programme is 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 learners with SEND.
- Learners will be helped and supported to understand the need for the learner acceptable use agreement and encouraged to adopt safe and responsible use both within and outside school. Acceptable use is reinforced across the curriculum, with opportunities to discuss how to act within

moral and legal boundaries online, with reference to the Computer Misuse Act 1990. Lessons and further resources are available on the CyberChoices site.

- Staff will act as good role models in their use of digital technologies, the internet and mobile devices (as defined in the code of conduct)
- In lessons where internet use is pre-planned, learners will 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 learners are allowed to freely search the internet, staff will be vigilant in supervising the learners and monitoring the content of the websites the young people visit
- The online safety education programme will be relevant and up to date to ensure the quality of learning and outcomes**.**

Contribution of learners

At Witham St Hughs Academy we acknowledge, learn from, and use the skills and knowledge of learners in the use of digital technologies. We recognise the potential for this to shape the online safety strategy for our Academy community and how this contributes positively to the personal development of young people. Their contribution is recognised through:

- mechanisms to canvass learner feedback and opinion.
- appointment of digital leaders and curriculum champions
- learners contributing to the online safety education programme e.g. peer education, digital leaders leading assemblies across school, online safety lessons
- learners designing/updating acceptable user agreements
- contributing to online safety events with the wider Academy community e.g. parents' evenings, family learning programmes etc.

Staff/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 Academy or college safeguarding approach and wider staff training and curriculum planning.**"***

All staff will 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 delivered to all staff, at least annually. 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 Academy '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 our Academy online safety policy and acceptable use agreements. It will include explicit reference to classroom management, professional conduct, online reputation and the need to model positive online behaviours.
- the 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 (or other nominated person) will provide advice/guidance/training to individuals as required.

Governors

Governors should take part in online safety training/awareness sessions, with particular importance for those who are members of any sub-committee/group involved in technology/online safety/health and safety/safeguarding. This may be offered in several ways such as:

- attendance at training provided by the local authority/ trust or other relevant organisation
- participation in Academy level training / information sessions for staff or parents

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

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

Families

Parents and carers play an essential role in the education of their children and in the monitoring/regulation of their children's online behaviours. However, they may have a limited understanding of online safety risks and issues. 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.

At Witham St Hughs Academy we will seek to provide information and awareness to parents and carers through:

- regular communication, awareness-raising and engagement on online safety issues, curriculum activities and reporting routes
- regular opportunities for engagement with parents/carers on online safety issues through awareness workshops / parent/carer evenings etc

- the learners – who are encouraged to pass on to parents the online safety messages they have learned in lessons and by learners leading sessions at parent/carer evenings.
- letters, newsletters, website, learning platform,
- high profile events / campaigns e.g. Safer Internet Day
- reference to the relevant web sites/publications, e.g. SWGfL; www.saferinternet.org.uk/; www.childnet.com/parents-and-carers (see Appendix for further links/resources).
- Sharing good practice with other schools in clusters and or LA / Trust

Adults and agencies

At Witham St Hughs Academy we will provide opportunities for local community groups and members of the wider community to gain from the Academy 's online safety knowledge and experience. This may be offered through the following:

- online safety messages targeted towards families and relatives.
- providing family learning courses in use of digital technologies and online safety
- providing online safety information via our website and social media for the wider community
- supporting community groups, e.g. early years settings, childminders, youth/sports/voluntary groups to enhance their online safety provision

Technology

The DfE Filtering and Monitoring Standards states that "Your IT service provider may be a staff technician or an external service provider".

We at Witham St Hughs Academy use our internal IT Support Function known as L.E.A.D. IT Services as our IT service provider. We are aware that it is our responsibility to ensure that they carry out all the online safety and security measures that would otherwise be the responsibility of the Academy. We ensure that L.E.A.D. I.T Services and the internal IT team are fully aware of the Academy Online Safety Policy/acceptable use agreements.

The Academy and the L.E.A.D. IT Services team are responsible for ensuring that the technical infrastructure/network is as safe and secure as is reasonably possible and that processes and procedures approved within this policy are implemented. We will 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. A more detailed technical security statement can be found in the Appendices.

Filtering and monitoring

The DfE guidance (for England) on filtering and monitoring in KCSIE" states:

> *"It is essential that governing bodies and proprietors ensure that appropriate filtering and monitoring systems are in place ...governing bodies and proprietors should be doing all that they reasonably can to limit children's exposure to the … risks from the school's or college's IT system. As part of this process, governing bodies and proprietors should ensure their Academy or college has appropriate filtering and*

monitoring systems in place and regularly review their effectiveness. They should ensure that the leadership team and relevant staff have an awareness and understanding of the provisions in place and manage them effectively and know how to escalate concerns when identified…

The appropriateness of any filtering and monitoring systems are a matter for individual schools and colleges and will be informed in part, by the risk assessment required by the Prevent Duty. To support schools and colleges to meet this duty, the Department for Education has published filtering and monitoring standards…"

Our Academy filtering and monitoring provision is agreed by senior leaders, governors and L.E.A.D. I.T Services and 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 L.E.A.D. I.T Services will have technical responsibility for ensuring the filtering and monitoring provision is reviewed (at least annually) by senior leaders, the Designated Safeguarding Lead and a governor with the involvement of the L.E.A.D. I.T Services.

- checks on the filtering and monitoring system are carried out by L.E.A.D. I.T Services with the involvement of a senior leader, the Designated Safeguarding Lead and a governor, in particular when a safeguarding risk is identified, there is a change in working practice, e.g. remote access or BYOD or new technology is introduced.

Filtering

- Witham St Hughs Academy manages access to content across its systems for all users and on all devices using the Academy 's 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 (see Appendix for more details).
- filtering logs are regularly reviewed and alert the Designated Safeguarding Lead to breaches of the filtering policy, which are then acted upon.
- our Academy has (if possible) 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 Academy has a mobile phone statement (appendix C2) and where personal mobile devices have internet access through the Academy network, content is managed in ways that are consistent with 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 policy and practice.
- Websites using the new ECH (Encrypted Client Hello) standard are monitored through filtering that is installed on the device. Devices which are accessing the academies internet through a BYOD/Captive portal must install security certificates to ensure adequate filtering is in place. L.E.A.D. IT Services team will provide this certificate per Academy and support the rollout on request.

Monitoring

Witham St Hughs Academy has monitoring systems in place to protect the school, systems and users:

- We monitor all network use across all our 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.

Witham St Hughs Academy follows the UK Safer Internet Centre Appropriate Monitoring guidance and protects users and Academy systems through the use of the appropriate blend of strategies informed by our risk assessment. These may include:

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

Technical security

Witham St Hughs Academy technical systems will be managed in ways that ensure that we meet recommended technical requirements as a minimum

- responsibility for technical security resides with SLT who may delegate activities to identified roles.
- all users have clearly defined access rights to Academy technical systems and devices. Details of the access rights available to groups of users will be recorded by L.E.A.D. I.T Services and will be reviewed, at least annually, by the SLT

- password policy and procedures are implemented (consistent with guidance from the National Cyber Security Centre)
- 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 Academy networks and system will be protected by secure passwords. Passwords must not be shared with anyone.
- the administrator passwords for Academy systems are kept in a secure place, e.g. Academy safe.
- there is a risk-based approach to the allocation of learner usernames and passwords
- there will be regular reviews and audits of the safety and security of Academy technical systems
- 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 Academy systems and data. These are tested regularly. The Academy 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,
- L.E.A.D. I.T Services are responsible for ensuring that all software purchased by and used by the Academy 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 Academy devices out of the Academy and by family members is regulated by an acceptable use agreement that a user consents to when the device is allocated to them
- personal use of any device on the Academy network is regulated by acceptable use agreements that a user consents to when using the network
- staff members are not permitted to install software on Academy -owned devices
- removable media is not permitted unless approved by the SLT/L.E.A.D. IT Services
- systems are in place to control and protect personal data and data is encrypted at rest and in transit. (See personal data statement in the appendices for further detail)
- mobile device security and management procedures are in place (where mobile devices are allowed access to Academy systems).
- guest users are provided with appropriate access to Academy systems based on an identified risk profile and if required.

Mobile technologies

The DfE guidance "Keeping Children Safe in Education" states:

> *"The Academy or college should have a clear policy on the use of mobile and smart technology. Amongst other things this will reflect the fact many children have unlimited and unrestricted access to the internet via mobile phone networks (i.e. 3G, 4G and 5G). This access means some children, whilst at Academy or college, sexually harass, bully, and control others via their mobile and smart technology, share indecent images consensually and non-consensually (often via large chat groups) and view and share pornography and other harmful content. Schools and colleges should carefully consider how this*

is managed on their premises and reflect this in their mobile and smart technology policy and their child protection policy.

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

All users should be made aware that the primary purpose of the use of mobile/personal devices in an Academy context is educational. This policy will be consistent with and inter-related to other relevant Academy polices including but not limited to those for safeguarding, behaviour, anti-bullying, acceptable use, and policies around theft or malicious damage. Teaching about the safe and appropriate use of mobile technologies should be an integral part of the Academy 's online safety education programme.

A range of mobile technology strategies is possible. However, these need to be thoroughly researched, risk assessed and aligned with existing policy prior to implementation. A more detailed mobile technologies statement can be found in the Appendices.

Witham St Hughs Academy acceptable use agreements for staff, learners, parents, and carers outline the expectations around the use of mobile technologies.

We allow:

	Academy devices			**Personal devices**		
	Academy owned for individual use	Academy owned for multiple users	Authorised device[1]	Student owned	Staff owned	Visitor owned
Allowed in school	Yes	Yes	Yes	Yes (Y5 and Y6 only)	Yes	Yes
Full network access	Yes	Yes	Yes	No	No	No
Internet only	Yes	Yes	Yes	No	Yes	Yes

[1] Authorised device – purchased by the learner/family through a school-organised scheme. This device may be given full access to the network as if it were owned by the school.

Academy owned/provided devices:

- all Academy devices are managed though the use of Mobile Device Management software
- there is an asset log that clearly states whom a device has been allocated to. There is clear guidance on where, when and how use is allowed
- any designated mobile-free zone is clearly signposted
- personal use (e.g. online banking, shopping, images etc.) is clearly defined and expectations are well-communicated.
- the use of devices on trips/events away from the Academy is clearly defined and expectation are well-communicated.
- liability for damage aligns with current Academy policy for the replacement of equipment.
- education is in place to support responsible use.

Personal devices:

- there is a clear procedure covering the use of personal devices on Academy premises for all users
- where devices are used to support learning, staff have been trained in their planning, use and implementation, ensuring that all learners can access a required resource.
- where personal devices are brought to Witham St Hughs Academy, but their use is not permitted, appropriate, safe and secure storge should be made available.
- use of personal devices for Academy business is defined in the acceptable use agreements and staff handbook. Personal devices commissioned onto the Academy network are segregated effectively from Academy -owned systems
- the expectations for taking/storing/using images/video aligns with the Academy ’s acceptable use agreements and use of images/video statement. The non-consensual taking/using of images of others is not permitted.
- liability for loss/damage or malfunction of personal devices is clearly defined
- there is clear advice and guidance at the point of entry for visitors to acknowledge Academy requirements
- education about the safe and responsible use of mobile devices is included in the Academy online safety education programmes

Social media

With widespread use of social media for professional and personal purposes, we have a policy that sets out clear guidance for staff to manage risk and behaviour online.

Expectations for teachers’ professional conduct are set out in the DfE Teachers Standards but all adults working with children and young people at Witham St Hughs Academy must understand that the nature and responsibilities of their work place them in a position of trust and that their conduct should reflect this.

We all have a duty of care to provide a safe learning environment for learners and staff. We could be held responsible, indirectly for acts of our employees in the course of their employment. Staff members who harass,

bully online, discriminate on the grounds of any protected characteristic or who defame a third party in the course of their duties may render the Academy liable to the injured party. Reasonable steps to prevent predictable harm are in place.

Witham St Hughs Academy provides the following measures to ensure reasonable steps are in place to minimise risk of harm to learners 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 will ensure that:

- No reference should be made in social media to learners, parents/carers or Academy staff.
- They do not engage in online discussion on personal matters relating to members of the Academy community.
- personal opinions should not be attributed to the Academy.
- security settings on their personal social media profiles are regularly checked to minimise risk of loss of personal information.
- they act as positive role models in their use of social media

When official Academy social media accounts are established, there is:

- a process for approval
- clear processes for the administration, moderation, and monitoring of these accounts – involving at least two members of staff
- a code of behaviour for users of the accounts
- systems for reporting and dealing with abuse and misuse
- understanding of how incidents may be dealt with under Academy disciplinary procedures.

Personal use

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

Monitoring of public social media

- As part of active social media engagement, we may pro-actively monitor the Internet for public postings about Witham St Hughs Academy.
- when parents/carers express concerns about our Academy on social media we will urge them to make direct contact with the Academy, in private, to resolve the matter. Where this cannot be resolved, parents/carers will be directed to the Academy complaints procedure.

At Witham St Hughs Academy, use of social media for professional purposes will be checked regularly by a senior leader or another appointed senior member of staff to ensure compliance with the social media, data protection, communications, digital image and video policies. In the event of any social media issues that the Academy is unable to resolve support may be sought from the Professionals Online Safety Helpline.

The social media statement in Appendix C4 provides more detailed guidance on our responsibilities and on good practice.

Digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and learners instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and learners need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for online bullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. At Witham St Hughs Academy, we will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm.

- we may use live-streaming or video-conferencing services in line with national and local safeguarding guidance / policies. Guidance can be found on the SWGfL Safer Remote Learning web pages and in the DfE Safeguarding and remote education
- when using digital images, staff will inform and educate learners about the risks associated with the taking, use, sharing, publication and distribution of images
- Staff and volunteers must be aware of learners whose images must not be taken or published. All images should be taken only on Academy devices. The personal devices of staff must not be used for such purposes
- Parents/carers are not permitted to take videos and digital images of their children or others at Academy events for their own personal use to respect everyone's privacy and in some cases protection, (as such use in not covered by the Data Protection Act).
- staff are allowed to take digital/video images to support educational aims, but must follow our procedures concerning the sharing, storage, distribution and publication of those images
- care should be taken when sharing digital/video images that learners are appropriately dressed
- learners must not take, use, share, publish or distribute images of others without their permission
- photographs published on the website, or elsewhere that include learners will be selected carefully and will comply with Online Safety Policy

- learners' 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 learners are taken for use in our Academy or published on the Academy website/social media. (see parents and carers acceptable use agreement in the Appendix). Permission is not required for images taken solely for internal purposes
- parents/carers will be informed of the purposes for the use of images, how they will be stored and for how long – in line with the Academy data protection policy
- images will be securely stored in line with the Academy retention policy
- learners' work can only be published with the permission of the learner and parents/carers.

AI Artificial Intelligence

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Microsoft Co-Pilot.

Witham St Hughs Academy recognises that AI has many uses to help pupils learn but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.

Staff are encouraged to stay informed about the latest developments in AI technologies and to engage in ongoing professional development to understand both the benefits and risks associated with these tools. By doing so, they can better support learners in navigating the digital landscape responsibly and ethically.

It is essential to establish clear guidelines and protocols for the use of AI within the Academy, ensuring that all stakeholders are aware of the potential implications and the necessary precautions to mitigate any negative impacts. This includes regular monitoring and evaluation of AI tools to ensure they align with our educational goals and values.

Witham St Hughs Academy will treat any use of AI to bully pupils in line with our anti-bullying/behaviour policy.

Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used by the trust.

In summary, while AI presents exciting opportunities for enhancing learning experiences, it is imperative to approach its integration with caution and a commitment to safeguarding the well-being of all members of the Academy community. Through collaborative efforts and a proactive approach, we can harness the potential of AI to foster a positive and inclusive learning environment.

Online publishing

Witham St Hughs Academy communicates with parents/carers and the wider community, and promotes the Academy through:

- Public-facing website
- Social media
- Online newsletters

Our website is managed/hosted by LEAD IT. We ensure that the 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 Academy calendars and personal information – ensuring that there is least risk to members of the Academy community, through such publications.

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

At Witham St Hughs Academy, we ensure our online publishing provides information about online safety e.g., publishing the Academy 's Online Safety Policy and acceptable use agreements; curating latest advice and guidance; news articles etc, creating an online safety page on the Academy website.

The website includes an online reporting process for parents and the wider community to register issues and concerns to complement the internal reporting process. (Report CEOP button)

Data protection

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

Witham St Hughs Academy:

- has a Data Protection Policy.
- implements the data protection principles and can demonstrate that it does so
- has paid the appropriate fee to the Information Commissioner's Office (ICO)
- has appointed an appropriate Data Protection Officer (DPO) who has effective understanding of data protection law and is free from any conflict of interest. Our Academy also has a Manager and Systems Controllers to support the DPO
- has a 'Record of Processing Activities' in place and knows exactly what personal data is held, where, why and which member of staff has responsibility for managing it
- the Record of Processing Activities lists the lawful basis for processing personal data (including, where relevant, consent). Where special category data is processed, an additional lawful basis is listed
- has an 'information asset register' in place and knows exactly what personal data is held, where, why and which member of staff has responsibility for managing it
- information asset register lists the lawful basis for processing personal data (including, where relevant, consent). Where special category data is processed, an additional lawful basis will have also been listed

- will hold the minimum personal data necessary to enable it to perform its function and will not hold it for longer than necessary for the purposes it was collected for. The Academy 's 'retention schedule" supports this.
- data held is accurate and up to date and is held only for the purpose specified. Systems are in place to identify inaccuracies, such as asking parents to check emergency contact details at suitable intervals
- provides staff, parents, volunteers, teenagers, and older children with information about how the Academy looks after their data and what their rights are in a clear Privacy Notice (see Privacy Notice section in the appendix)
- has procedures in place to deal with the individual rights of the data subject, e.g. one of the dozen rights applicable is that of Subject Access which enables an individual to see/have a copy of the personal data held about them
- carries out Data Protection Impact Assessments (DPIA) where necessary e.g. to ensure protection of personal data when accessed using any remote access solutions, or entering into a relationship with a new supplier
- has undertaken appropriate due diligence and has data protection compliant contracts in place with any data processors
- understands how to share data lawfully and safely with other relevant data controllers.
- has clear and understood policies and routines for the deletion and disposal of data
- reports any relevant breaches to the Information Commissioner within 72 hrs of becoming aware of the breach as required by law. It also reports relevant breaches to the individuals affected as required by law. In order to do this, it has a policy for reporting, logging, managing, investigating and learning from information risk incidents
- has a Freedom of Information procedure held within the GDPR policy
- provides data protection training for all staff at induction and appropriate refresher training thereafter. Staff undertaking particular data protection functions, such as handling requests relating to individual rights, will receive training appropriate for their function as well as the core training provided to all staff

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

- data will be encrypted, and password protected.
- device will be password protected.
- device will be protected by up-to-date endpoint (anti-virus) software
- data will be securely deleted from the device, in line with Academy policy (below) once it has been transferred or its use is complete.

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
- can recognise a possible breach, understand the need for urgency and know who to report it to within the Academy

- can help data subjects understand their rights and know how to handle a request whether verbal or written and know who to pass it to
- only use encrypted data storage for personal data
- will not transfer any Academy personal data to personal devices. Academies have access to VPN and web remote access services to allow remote working safely and securely.
- 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, a secure email account (where appropriate), and secure password protected devices.

The Personal Data Advice and Guidance in the appendix (C2) provides more detailed information on our Academy 's responsibilities and on good practice.

Outcomes

The impact of the Online Safety Policy and practice is regularly evaluated through the review/audit of online safety incident logs; behaviour/bullying reports; surveys of staff, learners; parents/carers and is reported to relevant groups:

- there is balanced professional debate about the evidence taken from the reviews/audits and the impact of preventative work e.g., online safety education, awareness, and training
- there are well-established routes to regularly report patterns of online safety incidents and outcomes to Academy leadership and Governors
- parents/carers are informed of patterns of online safety incidents as part of the Academy 's online safety awareness raising
- online safety (and related) policies and procedures are regularly updated in response to the evidence gathered from these reviews/audits/professional debate
- the evidence of impact is shared with other academies, agencies and LAs to help ensure the development of a consistent and effective local online safety strategy.

Appendix

The appendices are as follows:

A1 - Learner Acceptable Use Agreement – KS2
A2 - Learner Acceptable Use Agreement – for younger learners (Foundation/KS1)
A3 - Parent/Carer Acceptable Use Agreement
A4 - Staff (and Volunteer) Acceptable Use Agreement
A5 - Responding to incidents of misuse – flow chart
A6 - Record of reviewing devices/internet sites (responding to incidents of misuse)
A7 - Reporting Log
B1 - Training Needs Audit Log
C1 - Technical Security statement (including filtering and passwords)
C2 - Personal Data Advice and Guidance
C3 – Academy Online Safety statement; Electronic Devices - Searching Screening and Confiscation (new DfE guidance from September 2022)
C4 - Mobile Technologies statement (inc. BYOD/BYOT)
C5 - Social Media statement
Legislation
Links to other organisations and resources
Glossary of Terms

A1 Learner acceptable use agreement template – for KS2

Introduction

Digital technologies have become integral to the lives of children and young people, both within and outside academies. These technologies are powerful tools, which open-up new opportunities for everyone. They can stimulate discussion, encourage creativity, and stimulate awareness of context to promote effective learning. Learners should have an entitlement to safe access to these digital technologies.

This acceptable use agreement is intended:

- to ensure that learners will have good access to devices and online content, be responsible users and stay safe while using digital technologies for educational, personal and recreational use
- to help learners understand good online behaviours that they can use in school, but also outside Academy
- to protect Academy devices and networks from accidental or deliberate misuse that could put the security of the systems and users at risk.

Acceptable use agreement

When I use devices, I must behave responsibly to help keep me and other users safe online and to look after the devices.

For my own personal safety:

- I understand that what I do online will be supervised and monitored and that I may not be allowed to use devices in Academy unless I follow these rules and use them responsibly.
- I will only visit internet sites that adults have told me are safe to visit.
- I will keep my username and password safe and secure and not share it with anyone else.
- I will be aware of “stranger danger” when I am online.
- I will not share personal information about myself or others when online.
- If I arrange to meet people off-line that I have communicated with online, I will do so in a public place and take a trusted adult with me.
- I will immediately tell an adult if I see anything that makes me feel uncomfortable when I see it online.

I will look after the devices I use, so that the Academy and everyone there can be safe:

- I will handle all the devices carefully and only use them if I have permission.
- I will not try to alter the settings on any devices or try to install any software or programmes.
- I will tell an adult if a device is damaged or if anything else goes wrong.
- I will only use the devices to do things that I am told to do by an adult.

I will think about how my behaviour online might affect other people:

- When online, I will act as I expect others to act toward me.
- I will not copy anyone else’s work or files without their permission.

- I will be polite and responsible when I communicate with others, and I appreciate that others may have different opinions to me.
- I will not take or share images of anyone without their permission.

I know that there are other rules that I need to follow:

- I will only use my own personal devices (mobile phones/smart watches.) when off then Academy site or if I have permission if I am allowed, I still have to follow all the other Academy rules if I use them.
- Where work is protected by copyright, I will not try to download copies (including music and videos).
- When I am using the internet to find information, I should take care to check that the information is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.
- I should have permission if I use the original work of others in my own work.

I understand that I am responsible for my actions, both in and out of school:

- I know that I am expected to follow these rules in our Academy and that I should behave in the same way when out of our Academy as well.
- I understand that if I do not follow these rules, I may be subject to disciplinary action. This could include *loss of access to the Academy network/internet, suspensions, parents/carers contacted and in the event of illegal activities involvement of the police.*

Learner Acceptable Use Agreement Form

Please complete the sections below to show that you have read, understood and agree to the rules included in the acceptable user agreement. If you do not sign and return this agreement, access will not be granted to Academy systems. Children will be made aware of the user agreement during a class computing session and a member of staff delivering will sign on behalf of all children present.

I have read and understand the above and agree to follow these guidelines when:

- I use the Academy systems and devices (both in and out of school)
- I use my own devices in the Academy (when allowed) e.g. mobile phones, gaming devices USB devices, cameras etc.
- I am out of Academy and involved in any online behaviour that might affect the Academy or other members of the school.

Class:.....

Signed (staff on behalf of the children present): .....

Date: .....

A2 Learner acceptable use agreement template – for younger learners (Foundation/KS1)

This is how we stay safe when we use computers:

- I will ask a teacher or suitable adult if I want to use the computers/tablets.
- I will only use activities that a teacher or suitable adult has told or allowed me to use.
- I will take care of computers/tablets and other equipment.
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong.
- I will tell a teacher or suitable adult if I see something that upsets me on the screen.
- I know that if I break the rules, I might not be allowed to use a computer/tablet.

Children will be made aware of the user agreement during a class computing session and a member of staff delivering will sign on behalf of all children present.

Class:.....

Signed (staff on behalf of the children present): .....

Date: .....

A3 Parent/carer acceptable use agreement template

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies provide powerful tools, which open new opportunities for everyone. They can stimulate discussion, promote creativity, and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This acceptable use policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that Academy systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that parents and carers are aware of the importance of online safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

The Academy will try to ensure that learners have good access to digital technologies to enhance their learning and will, in return, expect the learners to agree to be responsible users. A copy of the learner acceptable use agreement is attached to this permission form, so that parents/carers will be aware of the Academy expectations of the young people in their care.

Parents are requested to sign the permission form below to show their support of the Academy in this important aspect of the school's work.

Permission Form

Parent/Carers Name: .....

Learner Name: .....

As the parent/carer of the above learners, I give permission for my son/daughter to have access to the digital technologies at school.

Either: (KS2 and above)

I know that my son/daughter has agreed to follow the acceptable use agreement and has received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

Or: (KS1)

I understand that the Academy has discussed the acceptable use agreement with my son/daughter and that they have received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

I understand that the Academy will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and systems. I also understand that the Academy cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my son's/daughter's activity on the systems will be monitored and that the Academy will contact me if they have concerns about any possible breaches of the acceptable use agreement.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the Academy if I have concerns over my child's online safety.

As the schools is collecting personal data by issuing this form, it should inform parents/carers as to:

This form (electronic or printed)
Who will have access to this form.
Where this form will be stored.
How long this form will be stored for.
How this form will be destroyed.

Signed: .....

Date: .....

Use of Digital/Video Images

The use of digital/video images plays an important part in learning activities. Learners and members of staff may use digital cameras to record evidence of activities in lessons and out of school. These images may then be used in presentations in subsequent lessons.

Images may also be used to celebrate success through their publication in newsletters, on the Academy website and occasionally in the public media. Where an image is publicly shared by any means, only your child's first name will be used if relevant.

The Academy will comply with the Data Protection Act and request parent's/carer's permission before taking images of members of the school. We will also ensure that when images are published that the young people cannot be identified by the use of their names.

Parents/carers are requested to sign the permission form to allow the Academy to take and use images of their children and for the parents/carers to agree.

As the schools is collecting personal data by issuing this form, it should inform parents/carers as to:

This form (electronic or printed)	The images
Who will have access to this form.	Where the images may be published. Such as; Twitter, Facebook, the academies website, local press, etc. (see relevant section of form below)
Where this form will be stored.	Who will have access to the images.
How long this form will be stored for.	Where the images will be stored.
How this form will be destroyed.	How long the images will be stored for.
	How the images will be destroyed.
	How a request for deletion of the images can be made.

Digital/Video Images Permission Form

Parent/Carers Name:..... Learner Name:.....

As the parent/carer of the above learner, I agree to the Academy taking digital/video images of my child/children.	Yes/No
I agree to these images being used:	
• to support learning activities.	Yes/No
• in publicity that reasonably celebrates success and promotes the work of the school.	Yes/No
• On display in the classroom	Yes/No

Signed: .....

Date: .....

Use of Cloud Systems Permission Form

The Academy uses OneDrive for staff. This permission form describes the tools and learner responsibilities for using these services.

Seesaw is available to each learner as part of the school's online presence. Additionally, Year 6 will be using OneDrive for their computing units.

Seesaw is used throughout the Academy with the addition of Year 6s' access to the OneDrive for computing units. These platforms enable your child to collaboratively create, edit and share files and websites for Academy related projects. Seesaw accounts are entirely online and available 24/7 from any internet-connected computer, meanwhile OneDrive can only be accessed during the Academy hours, during their computing lessons.

The Academy believes that use of the tools significantly adds to your child's educational experience.

As the Academy is collecting personal data and sharing this with a third party, it should inform parents/carers about:

This form (electronic or printed)	The data shared with the service provider
Who will have access to this form.	What data will be shared

Where this form will be stored.	Who the data will be shared with
How long this form will be stored for.	Who will have access to the data.
How this form will be destroyed.	Where the data will be stored.
	How long the data will be stored for.
	How the data will be destroyed.
	How a request for deletion of the data can be made.

Do you consent to your child to having access to this service? Yes/No

Learner Name: ..... Parent/Carers Name: .....

Signed: ..... Date: .....

A4 Staff (and volunteer) acceptable use policy agreement template

Academy Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe access to the internet and digital technologies at all times.

This acceptable use policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that Academy systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of technology in their everyday work.

The Academy will try to ensure that staff and volunteers will have good access to digital technology to enhance their work, to enhance learning opportunities for learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use Academy systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that learners receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

For my professional and personal safety:

- I understand that the Academy will monitor my use of the Academy digital technology and communications systems.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email, VLE etc.) out of school, and to the transfer of personal data (digital or paper based) out of Academy
- I understand that the Academy digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using Academy systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.

- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language, and I appreciate that others may have different opinions.
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital/video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the Academy website/VLE) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use social networking sites in Academy in accordance with the school's policies.
- I will only communicate with learners and parents/carers using official Academy systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The Academy has the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my mobile devices in school, I will follow the rules set out in this agreement, in the same way as if I was using Academy equipment. I will also follow any additional rules set by the Academy about such use. I will ensure that any such devices are protected by up-to-date anti-virus software and are free from viruses.
- I will not use personal email addresses on the school's ICT systems.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will ensure that my data is regularly backed up, in accordance with relevant Academy policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, terrorist or extremist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in Academy policies.
- I will not disable or cause any damage to Academy equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the Academy Personal Data Policy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based documents containing personal data must be held in lockable storage.
- I understand that data protection policy requires that any staff or learner data to which I have access, will be kept private and confidential, except when I am required by law or by Academy policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software; however this may have happened.

When using the online systems in my professional capacity or for Academy sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work

- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of the school:

- I understand that this acceptable use policy applies not only to my work and use of school's digital technology equipment in school, but also applies to my use of Academy systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school
- I understand that if I fail to comply with this acceptable use agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors/Trustees and/or the Local Authority and in the event of illegal activities the involvement of the police and potential dismissal.

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 Academy 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					X

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
	• Using penetration testing equipment (without relevant permission)					
Users shall not undertake activities that are not illegal but are classed as unacceptable in Academy policies:	Accessing inappropriate material/activities online in a Academy setting including pornography, gambling, drugs. (Informed by the school's filtering practices and/or AUAs)			X	X	
	Promotion of any kind of discrimination				X	
	Using Academy systems to run a private business				X	
	Using systems, applications, websites or other mechanisms that bypass the filtering/monitoring or other safeguards employed by the Academy				X	
	Infringing copyright				X	X
	Unfair usage (downloading/uploading large files that hinders others in their use of the internet)			X	X	
	Any other information which may be offensive to others or breaches the integrity of the ethos of the Academy or brings the Academy into disrepute				X	

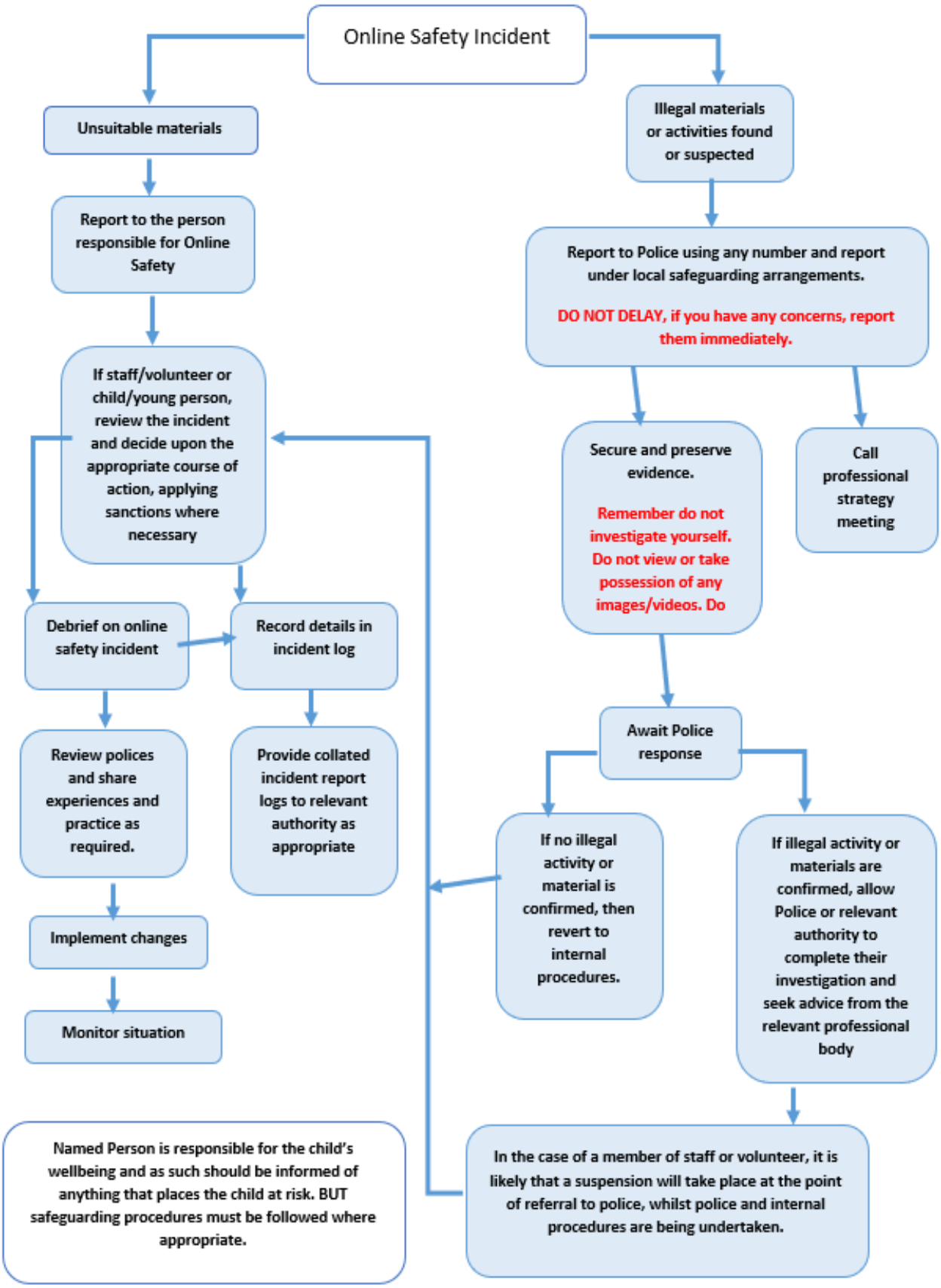
I have read and understand the above and agree to use the Academy digital technology systems (both in and out of school) and my own devices (in Academy and when carrying out communications related to the school) within these guidelines

Staff/Volunteer Name: .....

Signed: .....

Date: .....

A5 Responding to incidents of misuse – flow chart



A6 Record of reviewing devices/internet sites (responding to incidents of misuse) Upload to MyConcern or Confide as appropriate

Group: .....

Date: .....

Reason for investigation: .....

.....

.....

Details of first reviewing person

Name: .....

Position: .....

Signature: .....

Details of second reviewing person

Name: .....

Position: .....

Signature: .....

Name and location of computer used for review (for web sites)

.....

.....

Web site(s) address/device	Reason for concern

Conclusion and Action proposed or taken

A7 Reporting Log

Group: .....

Date	Time	Incident	Action Taken		Incident Reported By	Signature
			What?	By Whom?		

B1 Training needs audit log

Group: .....

Relevant training the last 12 months	Identified Training Need	To be met by	Cost	Review Date

C1 Academy technical security statement including filtering, monitoring and passwords)

Introduction

Effective technical security depends not only on technical measures, but also on appropriate policies and procedures and on good user education and training. This is informed by the Department for Education (DfE) guidance, and the Digital and Technology Standards. Our Academy will also ensure that we remain compliant with national, local authority or Trust guidance, as relevant. We are responsible for ensuring that the Academy infrastructure/network is as safe and secure as is reasonably possible and that:

- users can only access data to which they have right of access
- access to personal data is securely controlled in line with the Academy 's personal data policy
- system logs are maintained and reviewed to monitor user activity
- there is effective guidance and training for users
- there are regular reviews and audits of the safety and security of Academy computer systems, including filtering and monitoring provision

This statement is not designed to reproduce the entirety of the DfE's standards but is designed to support governors and senior leaders in the co-ordination of technical security. Governors and senior leaders remain responsible for the Academy 's technical security. L.E.A.D. IT Services have responsibility to ensure that Academies within the trust comply with the DfE guidelines and work with the DSLs to support the academies safeguarding requirements. It is also important that L.E.A.D. I.T Services works in partnership with the Designated Safeguarding Lead (DSL) to support the Academy safeguarding requirements. The Academy should also check their Local Authority/MAT/other relevant body policies/guidance on these technical issues.

Responsibilities

Education settings are directly responsible for ensuring they have the appropriate level of security protection procedures in place in order to safeguard their systems, staff and learners and reviewing the effectiveness of these procedures periodically to keep up with evolving cyber-crime technologies. The management of technical security is the responsibility of Governors and Senior Leaders, supported in this by the Designated Safeguarding Lead and L.E.A.D. I.T Services.

Statement

Witham St Hughs Academy is responsible for ensuring that their infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this statement are implemented. It will also need to ensure that the relevant people receive guidance and training and will be effective in carrying out their responsibilities:

- Academy technical systems will be managed in ways that ensure that we meet recommended technical requirements.
- cyber security is included in the Academy risk register.
- there will be regular reviews and audits of the safety and security of our Academy technical systems.
- servers, wireless systems, and cabling must be securely located and physical access restricted.
- there are rigorous and verified back-up routines, including the keeping of network-separated (air-gapped) copies off-site or in the cloud,
- appropriate security measures (including updates) are in place to protect the servers, firewalls, switches, routers, wireless systems, workstations, mobile devices etc from accidental or malicious attempts which might threaten the security of our Academy systems and data, including operating systems.
- The Academy 's infrastructure and individual workstations are protected by up-to-date software to protect against malicious threats from viruses, worms, trojans etc.
- responsibilities for the management of technical security are clearly assigned to appropriate and well-trained staff (this may be at our Academy, Trust or L.E.A.D I.T)
- all users will have clearly defined access rights to Academy technical systems and accounts will be deleted when the user leaves. Details of the access rights available to groups of users will be recorded by the network manager/technical staff/other person and will be reviewed, at least annually.
- users will be responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security *(see password section below)*
- L.E.A.D I.T Services, in partnership with Governors/SLT/DSL, regularly monitors and records the activity of users on our technical systems and users are made aware of this in the acceptable use agreement.
- mobile device security and management procedures are in place (where mobile devices are allowed access to Academy systems).
- an appropriate system is in place for users to report any actual/potential technical incident to the SLT/DSL.
- remote (classroom/network) management tools are used by staff to control workstations and view users' activity.
- guest users are provided with appropriate access to Academy systems based on an identified risk profile.
- by default, users do not have administrator access to any Academy -owned device.
- an agreed policy is in place regarding the extent of personal use that users (staff/learners/community users) and their family members are allowed on Academy devices that may be used out of the Academy.
- an agreed policy is in place regarding the use of removable media by users on Academy devices (see Academy personal data statement in the appendix for further detail)
- personal data cannot be sent over the internet or taken off the Academy site unless safely encrypted or otherwise secured. (see Academy personal data statement in the appendix for further detail)

Password Security

A safe and secure username/password system is essential if the above is to be established and will apply to all Academy technical systems, including networks, devices, email and learning platform).

Statement:

- The password policy and procedures reflect NCSC and DfE advice/guidance.
- The use of passwords is reduced wherever possible, for example, using Multi-Factor Authentication (MFA) or (Single Sign On) SSO.
- Security measures are in place to reduce brute-force attacks and common passwords are blocked.
- Academy networks and system will be protected by secure passwords.
- Passwords are encrypted by the system to prevent theft.
- Some passwords do not expire, so the use of password managers is encouraged.
- Complexity requirements (e.g. capital letter, lower case, number, special character) are not used.
- Users are able to reset their password themselves.
- It is recommended that all passwords are at least 12 characters long and users are encouraged to use 3 random words.
- Passwords are immediately changed in the event of a suspected or confirmed compromise.
- No default passwords are in use. All passwords provided “out of the box” are changed to a unique password by the IT Service Provider.
- All accounts with access to sensitive or personal data are protected by Multi-Factor Authentication methods.
- All users (adults and learners) have responsibility for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- Passwords must not be shared with anyone other than the IT team to perform support tasks, passwords shared with IT must be reset once support calls are resolved.

Learner passwords:

At Witham St Hughs Academy, we allocate year group usernames and passwords. With the addition of the allocation of Year 6 learner usernames and passwords for their OneDrive learning.

For younger children or those with special educational needs, the DfE guidance states that schools could:

- consider using authentication methods other than passwords, such as QR Codes.
- consider using a separate account accessed by the teacher rather than the student.
- consider if the Academy resource being accessed requires authentication or can it be shared without logging in.

Statements

- For younger children and those with special educational needs, learner usernames and passwords can be kept in an electronic or paper-based form, but they must be securely kept

when not required by the user. *Password complexity for these users could be reduced (for example 6-character maximum) and should not include special characters. Where external systems have different password requirements the use of random words or sentences should be encouraged.*

- Learners will be taught the importance of password security, this should include how passwords are compromised, and why these password rules are important. The Project EVOLVE Privacy and Security strand should help you with this.

Filtering and monitoring

Introduction to Filtering

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so, as online content changes dynamically and new technologies are constantly being developed. It is important, therefore, to understand that filtering is only one element in a larger strategy for online safety and acceptable use. Witham St Hughs Academy has a filtering policy to manage the associated risks and to provide preventative measures which are relevant to the situation in our Academy.

DfE Keeping Children Safe in Education requires schools to have "appropriate filtering".

Our filtering system is operational, up to date and applied to all:

- users, including guest accounts.
- Academy owned devices
- devices using the Academy broadband connection.

Our filtering system:

- filters all internet feeds, including any backup connections.
- is age and ability appropriate for the users and suitable for educational settings.
- Can handle multilingual web content, images, common misspellings and abbreviations.
- identifies technologies and techniques that allow users to get around the filtering such as VPNs and proxy services and block them.
- provides alerts when any web content has been blocked.

Introduction to Monitoring

Monitoring user activity on our devices is an important part of providing a safe environment for children and staff. Unlike filtering, it does not stop users from accessing material through internet searches or software. Monitoring allows us to review user activity on Academy devices. For monitoring to be effective it must pick up incidents urgently, usually through alerts or observations, allowing us to take prompt action and record the outcome.

Witham St Hughs Academy monitoring strategy is be informed by the filtering and monitoring review. A variety of monitoring strategies are used to minimise safeguarding risks on internet connected devices and may include:

- physically monitoring by staff watching screens of users
- live supervision by staff on a console with device management software
- network monitoring using log files of internet traffic and web access
- individual device monitoring through software or third-party services

Filtering and Monitoring Responsibilities

DfE Filtering Standards require that schools and colleges identify and assign roles and responsibilities to manage your filtering and monitoring systems, and include:

Role	Responsibility	Name / Position
Responsible Governor	Strategic responsibility for filtering and monitoring and need assurance that the standards are being met.	Miles Crawshaw
Senior Leadership	Team Member Responsible for ensuring these standards are met and: • procuring filtering and monitoring systems • documenting decisions on what is blocked or allowed and why • reviewing the effectiveness of your provision • overseeing reports Ensure that all staff: • understand their role • are appropriately trained • follow policies, processes and procedures • act on reports and concerns	Emily Broadley Michelle Dexter Hannah Younger Helen Patmore Leanne Riddell
Designated Safeguarding Lead	Lead responsibility for safeguarding and online safety, which could include overseeing and acting on: • filtering and monitoring reports • safeguarding concerns • checks to filtering and monitoring systems	Michelle Dexter Emily Broadley Hannah Younger
L.E.A.D I.T Services	Technical responsibility for: • maintaining filtering and monitoring systems • providing filtering and monitoring reports	Ian Wilson-Hart L.E.A.D I.T Services

	• completing actions following concerns or checks to systems	
All staff need to be aware of reporting mechanisms for safeguarding and technical concerns. They should report if:	• they witness or suspect unsuitable material has been accessed • they can access unsuitable material • they are teaching topics which could create unusual activity on the filtering logs • there is failure in the software or abuse of the system • there are perceived unreasonable restrictions that affect teaching and learning or administrative tasks • they notice abbreviations or misspellings that allow access to restricted material	

Statement

At Witham St Hughs Academy, internet access is filtered for all users. Differentiated internet access is available for staff and customised filtering changes are managed by L.E.A.D I.T Services. Illegal content is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation URL list and other illegal content lists. Filter content lists are regularly updated, and internet use is logged and frequently monitored. The monitoring process alerts our Academy to breaches of the filtering policy, which are then acted upon. There is a clear route for reporting and managing changes to the filtering system. Where personal mobile devices are allowed internet access through the Academy network, filtering will be applied that is consistent with our procedures.

- There is a filtering and monitoring system in place that safeguards staff and learners by blocking harmful, illegal and inappropriate content.
- There is a monitoring system that enables the prompt investigation of a potential safeguarding incident and outcomes are logged.
- Roles and responsibilities for the management of filtering and monitoring systems have been defined and allocated.
- The filtering and monitoring provision is reviewed at least annually and checked regularly.
- There is a defined and agreed process for making changes to the filtering or monitoring system that involves a senior leader in the agreement of the change.
- Mobile devices that access the Academy 's internet connection (whether Academy or personal devices) will be subject to the same filtering standards as other devices on our Academy systems.
- The Academy has provided enhanced/differentiated user-level filtering through the use of the iBOSS filtering system. (allowing different filtering levels for different ages/stages and different groups of users – staff/learners etc.)

Changes to filtering and monitoring systems

There is a clear process for requests to change the filtering and monitoring systems and who makes the decision to alter the filtering system.

In this section the Academy should provide a detailed explanation of:

- how, and to whom, users may request changes to the filtering and monitoring systems
- the grounds on which changes may be permitted or denied
- how a second responsible person will agree to the change before it is made
- any audit/reporting system

Filtering and monitoring review and checks

To understand and evaluate the changing needs and potential risks to our Academy, the filtering and monitoring provision will be reviewed at least annually. The review will be conducted by members of the senior leadership team, the designated safeguarding lead (DSL), and the L.E.A.D I.T Services. Additional checks to filtering and monitoring will be informed by the review process so that governors have assurance that systems are working effectively and meeting safeguarding obligations.

Reviewing the filtering and monitoring provision

A review of filtering and monitoring will be carried out to identify the current provision, any gaps, and the specific needs of learners and staff.

The review will take account of:

- the risk profile of learners, including their age range, pupils with special educational needs and disability (SEND), pupils with English as an additional language (EAL)
- what the filtering system currently blocks or allows and why
- any outside safeguarding influences, such as county lines
- any relevant safeguarding reports
- the digital resilience of learners
- teaching requirements, for example, the RHSE and PSHE curriculum
- the specific use of chosen technologies, including Bring Your Own Device (BYOD)
- what related safeguarding or technology policies are in place
- what checks are currently taking place and how resulting actions are handled

To make the filtering and monitoring provision effective, the review will inform:

- related safeguarding or technology policies and procedures
- roles and responsibilities
- training of staff

- curriculum and learning opportunities
- procurement decisions
- how often and what is checked
- monitoring strategies

The review will be carried out as a minimum annually, or when:

- a safeguarding risk is identified
- there is a change in working practice, e.g. remote access or BYOD
- new technology is introduced

Checking the filtering and monitoring systems

Checks to filtering and monitoring systems are completed and recorded as part of the filtering and monitoring review process. How often the checks take place will be based on the context, the risks highlighted in the filtering and monitoring review, and any other risk assessments. Checks will be undertaken from both a safeguarding and IT perspective.

When filtering and monitoring systems are checked this should include further checks to verify that the system setup has not changed or been deactivated. Checks are performed on a range of:

- Academy owned devices and services, including those used off site
- geographical areas across the site
- user groups, for example, teachers, pupils and guests

Logs of checks are kept so they can be reviewed. These record:

- when the checks took place
- who did the check
- what was tested or checked
- resulting actions

Training/Awareness:

It is a statutory requirement in England that staff receive training, at least annually, about safeguarding, child protection, online safety and filtering and monitoring. Furthermore, in order to protect personal and sensitive data, governors, senior leaders, staff and learners will receive training about information security and data protection, at least annually.

Governors, Senior Leaders and staff are made aware of the expectations of them:

- at induction
- at whole-staff/governor training

- through the awareness of policy requirements
- through the acceptable use agreements
- in regular updates throughout the year

Those with specific responsibilities for filtering and monitoring (Responsible Governor, DSL, or other relevant persons) will receive enhanced training to help them understand filtering and monitoring systems and their implementation and review.

Learners are made aware of the expectations of them:

- in lessons (through modelling and explanation)
- through the acceptable use agreements

Parents will be informed of the Academy 's filtering policy through the acceptable use agreement and through online safety awareness sessions/newsletter etc. (amend as relevant)

Audit/monitoring/reporting/review:

Governors/SLT/DSL will ensure that full records are kept of:

- Training provided
- User Ids and requests for password changes
- User logons
- Security incidents related to this policy
- Annual online safety reviews including filtering and monitoring
- Changes to the filtering system
- Checks on the filtering and monitoring systems

Further guidance

Schools in England (and Wales) are required "to ensure children are safe from terrorist and extremist material when accessing the internet in school, including by establishing appropriate levels of filtering".

Furthermore, the Department for Education's statutory guidance 'Keeping Children Safe in Education' obliges schools and colleges in England to "ensure appropriate filters and appropriate monitoring systems are in place and regularly review their effectiveness" and they "should be doing all that they reasonably can to limit children's exposure to the above risks from the school's or college's IT system" however, schools will need to "be careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding."

To further support schools and colleges in England, the Department for Education published Digital and Technology standards.

The UK Safer Internet Centre has produced guidance on "Appropriate Filtering and Monitoring"

SWGfL, on behalf of UK Safer Internet Centre and DfE, developed further Filtering and Monitoring | SWGfL information for schools and colleges, including a checklist alongside further support for Governors

SWGfL provides a site for schools to test their filtering to ensure that illegal materials cannot be accessed: SWGfL Test Filtering

C4 Mobile technologies statement (inc. BYOD/BYOT)

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

The absolute key to considering the use of mobile technologies is that the learners, staff and wider Academy community understand that the primary purpose of having their personal device at our Academy is educational and that this is irrespective of whether the device is Academy owned/provided or personally owned. The mobile technologies statement sits alongside a range of polices including but not limited to the online safety policy, safeguarding policy, anti-bullying policy, acceptable use agreements and the behaviour policy. Teaching about the safe and appropriate use of mobile technologies is included in the online safety education programme.

Considerations

There are a number of issues and risks to consider when implementing mobile technologies, these include security risks in allowing connections to our Academy network, filtering of personal devices, breakages and insurance, access to devices for all learners, avoiding potential classroom distraction, network connection speeds, types of devices, charging facilities, total cost of ownership

The Academy acceptable use agreements for staff, learners and parents/carers will give consideration to the use of mobile technologies.

We allow:

	Academy devices		**Personal devices**			
	Academy owned and allocated to a single user	Academy owned for use by multiple users	Authorised device[2]	Learner owned	Staff owned	Visitor owned
Allowed in the Academy	**Yes**	**Yes**	**Yes**	Yes – Y6	Yes	Yes
Full network access	Yes	Yes	Yes	No	No	No
Internet only	Yes	Yes	Yes	No	No	No
No network access						

Witham St Hughs Academy has provided technical solutions for the safe use of mobile technologies:

- All Academy devices are managed though the use of Mobile Device Management software
- Appropriate access control is applied to all mobile devices according to the requirements of the user (e.g Internet only access, network access allowed, shared folder network access)
- The Academy has addressed broadband performance and capacity to ensure that core educational and administrative activities are not negatively affected by the increase in the number of connected devices
- For all mobile technologies on the Academy network, filtering will be applied to the internet connection and attempts to bypass this are not permitted
- Appropriate exit processes are implemented for devices no longer used our Academy location or by an authorised user. These may include revoking the link between MDM software and the device, removing proxy settings, ensuring no sensitive data is removed from the network, uninstalling school-licenced software etc.
- All mobile devices on the Academy network are monitored
- The software/apps originally installed by us must remain on the Academy owned device in usable condition and be easily accessible at all times. From time to time the Academy may add software applications for use in a particular lesson. Periodic checks of devices will be made to ensure that users have not removed required apps
- Witham St Hughs Academy will ensure that devices contain the necessary apps for learning. Apps added by us will remain the property of Witham St Hughs Academy and will not be accessible to learners on authorised devices once they leave Witham St Hughs Academy any apps bought by the user on their own account will remain theirs.
- Where Witham St Hughs Academy device has been provided to support learning. It is expected that learners will bring devices to Witham St Hughs Academy as required.
- The changing of settings that would stop the device working as it was originally set up and intended to work is not permitted

When personal devices are permitted:

- Personal devices commissioned onto the Academy network are segregated effectively from Academy -owned systems.
- Personal devices are brought into the Academy entirely at the risk of the owner and the decision to bring the device into the Academy lies with the user (and their parents/carers) as does the liability for any loss or damage resulting from the use of the device in Academy
- The Academy accepts no responsibility or liability in respect of lost, stolen or damaged devices while at the Academy or on activities organised or undertaken by the Academy (the Academy recommends insurance is purchased to cover that device whilst out of the home)
- The Academy accepts no responsibility for any malfunction of a device due to changes made to the device while on the Academy network or whilst resolving any connectivity issues
- The Academy recommends that the devices are made easily identifiable and have a protective case to help secure them as the devices are moved around the school. Pass-codes or PINs should be set on personal devices to aid security
- The Academy is not responsible for the day-to-day maintenance or upkeep of the user's personal device such as the charging of any device, the installation of software updates or the resolution of hardware issues

Users are expected to act responsibly, safely and respectfully in line with current acceptable use agreements, in addition:

- Devices are not permitted in tests or exams
- there is clear advice and guidance at the point of entry for visitors to acknowledge Academy requirements
  - Users are responsible for keeping their device up to date through software, security and app updates.
  - Users are responsible for charging their own devices and for protecting and looking after their devices while in the Academy
  - Confiscation and searching – Witham St Hughs Academy has the right to take, examine and search any device that is suspected of unauthorised use, either technical or inappropriate.
  - Users should be mindful of the age limits for app purchases and use and should ensure they read the terms and conditions before use.
- The expectations for taking/storing/using images/video aligns with the Academy ’s acceptable use agreements and use of images/video statement. The non-consensual taking/using of images of others is not permitted.
  - Devices may be used in lessons in accordance with teacher direction
  - Staff owned devices should not be used for personal purposes during teaching sessions, unless in exceptional circumstances
  - Printing from personal devices will not be possible

C5 Social media statement

Social media (e.g. Facebook, Twitter, LinkedIn) is a broad term for any kind of online platform which enables people to directly interact with each other. However, some games, for example Minecraft or World of Warcraft and video sharing platforms such as You Tube have social media elements to them.

Witham St Hughs Academy recognises the numerous benefits and opportunities which a social media presence offers. Staff, parents/carers and learners are actively encouraged to find creative ways to use social media. However, there are some risks associated with social media use, especially around the issues of safeguarding, bullying and personal reputation. This statement aims to encourage the safe use of social media by the Academy, its staff, parents, carers and children.

Scope

This statement is subject to the Academy 's codes of conduct and acceptable use agreements.

This:

- Applies to all staff and to all online communications which directly or indirectly, represent our Academy.
- Applies to such online communications posted at any time and from anywhere**.**
- Encourages the safe and responsible use of social media through training and education
- Defines the monitoring of public social media activity pertaining to our Academy

Witham St Hughs Academy respects privacy and understands that staff and learners may use social media forums in their private lives. However, personal communications likely to have a negative impact on professional standards and/or Witham St Hughs Academy reputation are within the scope of this statement.

Professional communications are those made through official channels, posted on the Academy account or using our Academy name. All professional communications are within the scope of this statement.

Personal communications are those made via a personal social media account. In all cases, where a personal account is used which associates itself with, or impacts on, our Academy, it must be made clear that the member of staff is not communicating on behalf of our Academy with an appropriate disclaimer. Such personal communications are within the scope of this statement.

Personal communications which do not refer to or impact upon Witham St Hughs Academy are outside the scope of this statement.

Digital communications with learners are also considered. Staff may use online programmes such as SeeSaw to communicate with learners via an Academy account for teaching and learning purposes and will consider whether this is appropriate and consider the potential implications.

Organisational control

Roles & Responsibilities

- **SLT**
  - Facilitating training and guidance on Social Media use.
  - Developing and implementing the Social Media policy
  - Taking a lead role in investigating any reported incidents.
  - Making an initial assessment when an incident is reported and involving appropriate staff and external agencies as required.
  - Receiving completed applications for social media accounts
  - Approving account creation
- **Administrator/Moderator**
  - Create the account following SLT approval
  - Store account details, including passwords securely
  - Be involved in monitoring and contributing to the account
  - Control the process for managing an account after the lead staff member has left the organisation (closing or transferring)
- **Staff**
  - Knowing the contents of and ensuring that any use of social media is carried out in line with this and other relevant policies
  - Attending appropriate training
  - Regularly monitoring, updating and managing content he/she has posted via Academy accounts
  - Adding an appropriate disclaimer to personal accounts when naming the Academy

Process for creating new accounts

Witham St Hughs Academy community is encouraged to consider if a social media account will help them in their work. Anyone wishing to create such an account must present a business case to the Leadership Team which covers the following points: -

- The aim of the account
- The intended audience
- How the account will be promoted
- Who will run the account (at least two staff members should be named)
- Will the account be open or private/closed

Following consideration by the SLT an application will be approved or rejected. In all cases, the SLT must be satisfied that anyone running a social media account on behalf of the Academy has read and understood this policy and received appropriate training. This also applies to anyone who is not directly employed by the Academy, including volunteers or parents.

Monitoring

Witham St Hughs Academy accounts will be monitored regularly and frequently (preferably 7 days a week, including during holidays). Any comments, queries or complaints made through those accounts must be responded to within 24 hours during Academy working hours (or on the next

working day if received at a weekend or during Academy holidays) even if the response is only to acknowledge receipt. Regular monitoring and intervention are essential in case a situation arises where bullying or any other inappropriate behaviour arises on an Academy social media account.

Behaviour

- Witham St Hughs Academy requires that all users using social media adhere to the standard of behaviour as set out in this policy and other relevant policies.
- Digital communications by staff must always be professional and respectful and in accordance with this policy. Staff will not use social media to infringe the rights and privacy of others or make ill-considered comments or judgments about others. Witham St Hughs Academy social media accounts must not be used for personal gain. Staff must ensure that confidentiality is maintained on social media even after they leave the employment of our Academy.
- Users must declare who they are in social media posts or accounts. Anonymous posts are discouraged in relation to Academy activity.
- If a journalist makes contact about posts made using social media staff must follow the Academy media procedures before responding, by initially speaking to the headteacher.
- Unacceptable conduct, (e.g. defamatory, discriminatory, offensive, harassing content or a breach of data protection, confidentiality, copyright) will be considered extremely seriously by us and will be reported as soon as possible to a relevant senior member of staff, and escalated where appropriate.
- The use of social media by staff while at work may be monitored, in line with our policies. The Academy permits reasonable and appropriate access to private social media sites. However, where excessive use is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
- We will take appropriate action in the event of breaches of the social media statement. Where conduct is found to be unacceptable, we will deal with the matter internally. Where conduct is considered illegal, we will report the matter to the police and other relevant external agencies and may take action according to the disciplinary policy.

Legal considerations

- Users of social media should consider the copyright of the content they are sharing and, where necessary, should seek permission from the copyright holder before sharing.
- Users must ensure that their use of social media does not infringe relevant data protection laws, or breach confidentiality.

Handling abuse

- When acting on behalf of Witham St Hughs Academy, respond to harmful and / or offensive comments swiftly and with sensitivity.
- If a conversation turns and becomes offensive or unacceptable, users should block, report or delete other users or their comments/posts and should inform the audience exactly why the action was taken.
- If you feel that you or someone else is subject to abuse through online communications, then this action must be reported using the agreed Academy protocols.

Tone

The tone of content published on social media should be appropriate to the audience, whilst retaining appropriate levels of professional standards. Key words to consider when composing online content are:

- Engaging
- Conversational
- Informative
- Professional

Use of images

Images can be used providing the following guidelines are strictly adhered to.

- Permission to use any photos or video recordings will be sought in line with the Academy 's digital and video images statement. If anyone, for any reason, asks not to be filmed or photographed then their wishes should be respected.
- **Under no circumstances** will staff share or upload learner pictures online other than via official channels.
- Staff will exercise their professional judgement about whether an image is appropriate to share on our Academy social media accounts. Learners will be appropriately dressed, not be subject to ridicule and must not be on any Academy list of children whose images must not be published.
- If a member of staff inadvertently takes a compromising picture which could be misconstrued or misused, they must delete it immediately and refer themselves to the headteacher.

Personal use

- **Staff**
    - Personal communications are those made via a personal online account. In all cases, where a personal account is used which associates itself with the Witham St Hughs Academy or impacts on us, 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 Witham St Hughs Academy are outside the scope of this policy.
    - Where excessive or inappropriate personal use of social media in Witham St Hughs Academy is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
    - The Academy permits reasonable and appropriate access to private social media sites.
- **Learners**
    - Staff are not permitted to follow or engage with current or prior learners of the Academy on any personal social media account**.**

      Witham St Hughs Academy 's education programme should enable the learners to be safe and responsible users of social media.

- Learners are encouraged to comment or post appropriately about the Academy. Any offensive or inappropriate comments will be resolved by the use of the Academy 's behaviour policy

- **Parents/carers**
  - If parents/carers have access to our learning platform where posting or commenting is enabled, parents/carers will be informed about acceptable use.
  - we have an active parent/carer education programme which supports the safe and positive use of social media. This includes information on the website.
  - Parents/Carers are encouraged to comment or post appropriately about the Academy. In the event of any offensive or inappropriate comments being made, we will ask the parent/carer to remove the post and invite them to discuss the issues in person. If necessary, parents can be referred to the Academy 's complaints procedures.

Monitoring posts about Witham St Hughs Academy

- As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about our Academy.
- We will respond to social media comments made by others according to a defined policy or process.

Appendix

Managing your personal use of social media:

- "Nothing" on social media is truly private
- Social media can blur the lines between your professional and private life. Don't use the Academy logo and/or branding on personal accounts
- Check your settings regularly and test your privacy
- Keep an eye on your digital footprint
- Keep your personal information private
- Regularly review your connections – keep them to those you want to be connected to
- When posting online consider; Scale, Audience and Permanency of what you post
- If you want to criticise, do it politely.
- Take control of your images – do you want to be tagged in an image? What would children or parents say about you if they could see your images?
- Know how to report a problem

Managing Witham St Hughs Academy social media accounts

The do's

- Check with a senior leader before publishing content that may have controversial implications for our Academy
- Use a disclaimer when expressing personal views
- Make it clear who is posting content
- Use an appropriate and professional tone
- Be respectful to all parties

- Ensure you have permission to 'share' other peoples' materials and acknowledge the author
- Express opinions but do so in a balanced and measured manner
- Think before responding to comments and, when in doubt, get a second opinion
- Seek advice and report any mistakes using the Academy 's reporting process
- Consider turning off tagging people in images where possible
- Ensure the account is set up securely and the account can be transferred to another approved staff member in the event of the account holder leaving our Academy.

The don'ts

- Don't make comments, post content or link to materials that will bring our Academy into disrepute
- Don't publish confidential or commercially sensitive material
- Don't breach copyright, data protection or other relevant legislation
- Don't link to, embed or add potentially inappropriate content. Consider the appropriateness of content for any audience of Academy accounts.
- Don't post derogatory, defamatory, offensive, harassing or discriminatory content
- Don't use social media to air internal grievances

Computer Misuse Act 1990

This Act makes it an offence to:

- Erase or amend data or programs without authority.
- Obtain unauthorised access to a computer.
- "Eavesdrop" on a computer.
- Make unauthorised use of computer time or facilities.
- Maliciously corrupt or erase data or programs.
- Deny access to authorised users.

Academies may wish to view the National Crime Agency website which includes information about "Cyber crime – preventing young people from getting involved". Each region in England (& Wales) has a Regional Organised Crime Unit (ROCU) Cyber-Prevent team that works with schools to encourage young people to make positive use of their cyber skills. There is a useful summary of the Act on the NCA site.

Data Protection Act 1998

This protects the rights and privacy of individual's data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Act states that person data must be:

- Fairly and lawfully processed.
- Processed for limited purposes.
- Adequate, relevant and not excessive.
- Accurate.
- Not kept longer than necessary.

- Processed in accordance with the data subject's rights.
- Secure.
- Not transferred to other countries without adequate protection.

The Data Protection Act 2018:

Updates the 1998 Act, incorporates the General Data Protection Regulations (GDPR) and aims to:

- Facilitate the secure transfer of information within the European Union.
- Prevent people or organisations from holding and using inaccurate information on individuals. This applies to information regarding both private lives or business.
- Give the public confidence about how businesses can use their personal information.
- Provide data subjects with the legal right to check the information businesses hold about them. They can also request for the data controller to destroy it.
- Give data subjects greater control over how data controllers handle their data.
- Place emphasis on accountability. This requires businesses to have processes in place that demonstrate how they're securely handling data.
- Require firms to keep people's personal data safe and secure. Data controllers must ensure that it is not misused.
- Require the data user or holder to register with the Information Commissioner.

All data subjects have the right to:

- Receive clear information about what you will use their data for.
- Access their own personal information.
- Request for their data to be revised if out of date or erased. These are known as the right to rectification and the right to erasure
- Request information about the reasoning behind any automated decisions, such as if computer software denies them access to a loan.
- Prevent or query about the automated processing of their personal data.

Freedom of Information Act 2000

The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures.

Communications Act 2003

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Malicious Communications Act 1988

It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.

Regulation of Investigatory Powers Act 2000

It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to:

- Establish the facts;
- Ascertain compliance with regulatory or self-regulatory practices or procedures;
- Demonstrate standards, which are or ought to be achieved by persons using the system;
- Investigate or detect unauthorised use of the communications system;
- Prevent or detect crime or in the interests of national security;
- Ensure the effective operation of the system.
- Monitoring but not recording is also permissible to:
- Ascertain whether the communication is business or personal.
- Protect or support help line staff.
- The Academy reserves the right to monitor its systems and communications in line with its rights under this act.

Trademarks Act 1994

This provides protection for Registered Trademarks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trademarks must not be used without permission. This can also arise from using a Mark that is confusingly similar to an existing Mark.

Copyright, Designs and Patents Act 1988

It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. YouTube).

Telecommunications Act 1984

It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

Criminal Justice & Public Order Act 1994

This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they:

- Use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or

- Display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

Racial and Religious Hatred Act 2006

This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Protection of Children Act 1978

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison

Sexual Offences Act 2003

A grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff fall in this category of trust). Any person engaging in sexual intercourse with a child under the age of 13 commits the offence of rape.

Public Order Act 1986

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence. Children, Families and Education Directorate page 38 April 2007.

Obscene Publications Act 1959 and 1964

Publishing an “obscene” article is a criminal offence. Publishing includes electronic transmission.

Human Rights Act 1998

This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of "higher law", affecting all other laws. In the Academy context, human rights to be aware of include:

- The right to a fair trial
- The right to respect for private and family life, home and correspondence
- Freedom of thought, conscience and religion
- Freedom of expression
- Freedom of assembly
- Prohibition of discrimination
- The right to education

These rights are not absolute. The Academy is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.

The Education and Inspections Act 2006

Empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of learners when they are off the Academy site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.

The Education and Inspections Act 2011

Extended the powers included in the 2006 Act and gave permission for Headteachers (and nominated staff) to search for electronic devices. It also provides powers to search for data on those devices and to delete data.

(see template policy in these appendices and for DfE guidance - http://www.education.gov.uk/schools/learnersupport/behaviour/behaviourpolicies/f0076897/screening-searching-and-confiscation)

The Protection of Freedoms Act 2012

Requires academies to seek permission from a parent/carer to use Biometric systems

The Academy Information Regulations 2012

Requires schools to publish certain information on its website:

https://www.gov.uk/guidance/what-maintained-schools-must-publish-online

Serious Crime Act 2015

Introduced new offence of sexual communication with a child. Also created new offences and orders around gang crime (including CSE)

Criminal Justice and Courts Act 2015

Revenge porn – as it is now commonly known – involves the distribution of private and personal explicit images or video footage of an individual without their consent, with the intention of causing them embarrassment and distress. Often revenge porn is used maliciously to shame ex-partners. Revenge porn was made a specific offence in the Criminal Justice and Courts Act 2015. The Act specifies that if you are accused of revenge porn and found guilty of the criminal offence, you could be prosecuted and face a sentence of up to two years in prison.

For further guidance or support please contact the Revenge Porn Helpline

Links to other organisations or documents

The following links may help those who are developing or reviewing a Academy online safety policy and creating their online safety provision:

UK Safer Internet Centre

Safer Internet Centre – https://www.saferinternet.org.uk/
South West Grid for Learning - https://swgfl.org.uk/products-services/online-safety/
Childnet – http://www.childnet-int.org/
Professionals Online Safety Helpline - http://www.saferinternet.org.uk/about/helpline
Revenge Porn Helpline - https://revengepornhelpline.org.uk/
Internet Watch Foundation - https://www.iwf.org.uk/
Report Harmful Content - https://reportharmfulcontent.com/
Harmful Sexual Support Service

CEOP

CEOP - http://ceop.police.uk/
ThinkUKnow - https://www.thinkuknow.co.uk/

Others

LGfL – Online Safety Resources
Kent – Online Safety Resources page
INSAFE/Better Internet for Kids - https://www.betterinternetforkids.eu/
UK Council for Internet Safety (UKCIS) - https://www.gov.uk/government/organisations/uk-council-for-internet-safety

Tools for Schools / other organisations

Online Safety BOOST – https://boost.swgfl.org.uk/
360 Degree Safe – Online Safety self-review tool – https://360safe.org.uk/
360Data – online data protection self-review tool: www.360data.org.uk
SWGfL Test filtering - http://testfiltering.com/
UKCIS Digital Resilience Framework - https://www.gov.uk/government/publications/digital-resilience-framework
SWGfL 360 Groups – online safety self review tool for organisations working with children
SWGfL 360 Early Years - online safety self review tool for early years organisations

Bullying/Online-bullying/Sexting/Sexual Harassment

Enable – European Anti Bullying programme and resources (UK coordination/participation through SWGfL & Diana Awards) - http://enable.eun.org/
SELMA – Hacking Hate - https://selma.swgfl.co.uk
Scottish Anti-Bullying Service, Respectme - http://www.respectme.org.uk/
Scottish Government - Better relationships, better learning, better behaviour - http://www.scotland.gov.uk/Publications/2013/03/7388

DfE - Cyberbullying guidance -
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/374850/Cyberbullying_Advice_for_Headteachers_and_School_Staff_121114.pdf
Childnet – Cyberbullying guidance and practical PSHE toolkit:
http://www.childnet.com/our-projects/cyberbullying-guidance-and-practical-toolkit
Childnet – Project deSHAME – Online Sexual Harrassment
UKSIC – Sexting Resources
Anti-Bullying Network – http://www.antibullying.net/cyberbullying1.htm
Ditch the Label – Online Bullying Charity
Diana Award – Anti-Bullying Campaign

Social Networking

Digizen – Social Networking
UKSIC - Safety Features on Social Networks
Children's Commissioner, TES and Schillings – Young peoples' rights on social media

Curriculum

SWGfL Evolve - https://projectevolve.co.uk
UKCCIS – Education for a connected world framework
Department for Education: Teaching Online Safety in Schools

Teach Today – www.teachtoday.eu/
Insafe - Education Resources

Data Protection

360data - free questionnaire and data protection self review tool

ICO Guides for Organisations

IRMS - Records Management Toolkit for Schools

ICO Guidance on taking photos in schools

Professional Standards/Staff Training

DfE – Keeping Children Safe in Education
DfE - Safer Working Practice for Adults who Work with Children and Young People
Childnet – Academy Pack for Online Safety Awareness
UK Safer Internet Centre Professionals Online Safety Helpline

Infrastructure/Technical Support/Cyber-security

UKSIC – Appropriate Filtering and Monitoring
SWGfL Safety & Security Resources
Somerset - Questions for Technical Support
SWGfL - Cyber Security in Schools.
NCA – Guide to the Computer Misuse Act
NEN – Advice and Guidance Notes

Working with parents and carers

SWGfL – Online Safety Guidance for Parents & Carers
Vodafone Digital Parents Magazine
Childnet Webpages for Parents & Carers
Get Safe Online - resources for parents
Teach Today - resources for parents workshops/education
Internet Matters

Prevent

Prevent Duty Guidance
Prevent for schools – teaching resources
Childnet – Trust Me

Research

Ofcom –Media Literacy Research
Ofsted: Review of sexual abuse in schools and colleges

Further links can be found at the end of the UKCIS Education for a Connected World Framework

Glossary of Terms

AUP/AUA	Acceptable Use Policy/Agreement – see templates earlier in this document
CEOP	Child Exploitation and Online Protection Centre (part of National Crime Agency, UK Police, dedicated to protecting children from sexual abuse, providers of the Think U Know programmes.
CPD	Continuous Professional Development
FOSI	Family Online Safety Institute
ICO	Information Commissioners Office
ICT	Information and Communications Technology
INSET	In Service Education and Training
IP address	The label that identifies each computer to other computers using the IP (internet protocol)
ISP	Internet Service Provider
ISPA	Internet Service Providers' Association
IWF	Internet Watch Foundation
LA	Local Authority
LAN	Local Area Network
MAT	Multi Academy Trust
MIS	Management Information System
NEN	National Education Network – works with the Regional Broadband Consortia (e.g. SWGfL) to provide the safe broadband provision to schools across Britain.
Ofcom	Office of Communications (Independent communications sector regulator)
SWGfL	South West Grid for Learning Trust – the Regional Broadband Consortium of SW Local Authorities – is the provider of broadband and other services for schools and other organisations in the SW
TUK	Think U Know – educational online safety programmes for schools, young people and parents.
UKSIC	UK Safer Internet Centre – EU funded centre. Main partners are SWGfL, Childnet and Internet Watch Foundation.
UKCIS	UK Council for Internet Safety

VLE	Virtual Learning Environment (a software system designed to support teaching and learning in an educational setting,
WAP	Wireless Application Protocol

A more comprehensive glossary can be found at the end of the UKCIS Education for a Connected World Framework