Horizons Specialist Academy Trust
Providing infinite opportunities

Online Safety Policy

Adopted by: Resources & Audit & Risk Committee: 20 October 2026

Date of next review: Autumn 2027

Responsible Officer: Head of Estates & IT

Table of Contents

Scope of the Online safety Policy *2*

Equality Statement 2

Policy and leadership **3**

Responsibilities .....

Principals and senior leaders 3

Trustees & Governors 3

Designated Safety Lead (DSL) 4

Academy Online safety Lead (OSL) 5

Curriculum Leads 6

Teaching and support staff 6

IT Team 7

Learners 8

Parents and carers 8

Professional Standards *8*

Acceptable use *9*

Acceptable use agreements 9

User actions *9*

Reporting and responding *12*

Trust actions 15

The use of Artificial Intelligence (AI) systems in Trust .....

Staff/volunteers *15*

Families *16*

Student Voice *17*

Technology **17**

Filtering & Monitoring *18*

Managing the use of Mobile Phones, Smart Watches and other devices **20**

Social Networking, Social Media and Personal Publishing *21*

Sharing Nudes and Semi-Nudes: Responding to incidents and safeguarding children and young people **21**

Resources and support **22**

Helplines and reporting **23**

Advice and information for parents and carers **23**

Digital and video images *23*

Online Publishing *24*

Prevent Duty 25

Scope of the Online safety Policy

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

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

The online safety policy is supported by the following Trust Policies and other relevant guidance including:

- Acceptable Use Agreement
- Social Networking Policy
- Child Protection Policy
- Anti-bullying guidance
- Cyber Security Policy
- Information Security Policy
- Photography and Video Policy
- Keeping Children Safe in Education
- Filtering and Monitoring: core standard (DfE Meeting digital and technology standards in schools and colleges)
- Generative AI: product safety standards
- Sharing nudes and semi-nudes: advice for education settings working with children and young people
- Data protection policy
- Safe Use of AI Policy

Equality Statement

Horizons Specialist Academy Trust is committed to promoting equality, diversity and inclusion in all aspects of its work. We recognise and celebrate the diversity of our community and strive to ensure that all members — students, staff, parents, carers, trustees and visitors — are treated with dignity and respect, regardless of age, disability, gender identity or expression, race, religion or belief, sex, sexual orientation, pregnancy or maternity, or socio-economic background.

In implementing this Online Safety Policy, the Trust will ensure that no individual or group is treated less favourably or placed at a disadvantage because of a protected characteristic, and that reasonable adjustments are made to ensure equitable access for all.

This policy supports the Trust's commitment to eliminating discrimination, advancing equality of opportunity, and fostering good relations within our academies and the wider community.

Policy and leadership

Responsibilities

The Trust recognises that some children may be more vulnerable to harm online. Factors that may increase vulnerability include special educational needs and disabilities (SEND), communication difficulties, social isolation, mental health needs, care experience, family circumstances, previous trauma, exploitation, attendance concerns and other safeguarding vulnerabilities.

Everyone in the Trust community has a role in keeping children safe online. We work together to develop safe and responsible online behaviours, learn from each other and draw on good practice elsewhere. All members of the Trust community should report online safety concerns, inappropriate behaviour and misuse as soon as they become aware of them.

The following sections set out the specific online safety roles and responsibilities of individuals and groups within the Trust.

Principals and senior leaders

- The Principal has a duty of care for ensuring the safety (including online safety) of members of the Trust community 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 Principal and (at least) another member of the senior leadership team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.
- The Principal/senior leaders are responsible for ensuring that the Designated Safeguarding Lead / Online Safety Lead, IT provider/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 Principal/senior leaders will ensure that there is a system in place to allow for monitoring and support of those in Trust who carry out the internal online safety monitoring role.
- The Principal/senior leaders will work with the responsible Trustee, the Trust designated safeguarding lead (DSL) and IT service providers in all aspects of filtering and monitoring.

Trustees & 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 Trust 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)"

Trustees are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy.

This review will be carried out by Trustees. A member of the Trustees will take on the role of safeguarding Trustee to include:

- regular meetings with the Designated Safeguarding Lead / Online Safety Lead
- regularly receiving filtering & monitoring reports.
- 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, Trust DSL, and the IT Team and involve the responsible Trustee) - in-line with the DfE Filtering and Monitoring Standards
- reporting to relevant Board meeting

The Trustees will also support the Trust 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 an 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"
>
> *The Trust recognises that some children may be more vulnerable online, including children with SEND, looked after children, previously looked after children, children experiencing mental health difficulties and children who have experienced abuse, neglect or exploitation.*

While the responsibility for online safety is held by the DSL and cannot be delegated, the Trust may choose to appoint other relevant persons to work in support of the DSL in carrying out these responsibilities.

The DSL with support from the Trust Safeguarding Lead 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 Trust Safeguarding Lead to discuss current issues, review incidents and filtering and monitoring logs and ensuring that annual (at least) filtering and monitoring checks are carried out
- report regularly to Principal/senior leadership team
- be responsible for receiving reports of online safety incidents and handling them, and deciding whether to make a referral by liaising with relevant agencies, ensuring that all incidents are recorded.
- liaise with staff and the IT Team on matters of safety and safeguarding and welfare (including online and digital safety)

Academy Online safety Lead (OSL)

The Academy Online safety Lead will:

- work closely with the Designated Safeguarding Lead (DSL), (where these roles are not combined)
- receive reports of online safety issues, being aware of the potential for serious child protection concerns and ensure that these are logged to inform future online safety developments
- promote an awareness of and commitment to online safety education / awareness raising across the academies and beyond
- liaise with curriculum leaders to ensure that the online safety curriculum is planned, mapped, embedded and evaluated
- provide (or identify sources of) training and advice for staff/parents/carers/learners
- liaise with (Trust/local authority/MAT/external provider) technical staff, pastoral staff and support staff (as relevant)
- receive regularly updated training to allow them to understand how digital technologies are used and are developing (particularly by learners), and support coordinated online safety education with regard to the areas defined In Keeping Children Safe in Education:
    - Content: exposure to illegal, inappropriate or harmful material.
    - Contact: harmful interactions with others online, including grooming, exploitation and radicalisation.

- Conduct: personal online behaviour that increases risk to themselves or others, including bullying, peer abuse and sharing of harmful content.
- Commerce: risks associated with online gambling, scams, financial exploitation, advertising and inappropriate commercial influences**.**

Curriculum Leads

Curriculum Leads will work with the DSL/OSL to develop planned and coordinated online safety education.

This may be provided through:

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

Teaching and support staff

All staff are responsible for ensuring that:

- they have an awareness of current online safety matters/trends and of the current Trust 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 follow all relevant guidance and legislation including, for example, Keeping Children Safe in Education and UK GDPR regulations
- all digital communications with learners, parents and carers and others should be on a professional level and only carried out using official Trust systems and devices (where staff use AI, they should only use Trust-approved AI services for work purposes which have been evaluated to comply with organisational security and oversight requirements)
- they immediately report any suspected misuse or problem to the DSL for investigation/action, in line with the Trust safeguarding procedures
- 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 use 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, mobile devices, cameras, etc., in lessons and other Trust 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.
- Where live streaming, remote learning, online tutoring or other virtual sessions are used, staff must follow Trust safeguarding procedures, use approved platforms and accounts, maintain appropriate professional boundaries, apply attendance and reporting arrangements, and ensure concerns arising during virtual sessions are reported promptly to the DSL.
- there is a zero-tolerance approach to incidents of online-bullying, sexual harassment, image-based abuse, coercive behaviour, online exploitation by peers, group-based online abuse, harmful sexual behaviour online, discrimination and hatred
- they model safe, responsible, and professional online behaviours in their own use of technology, including outside the Trust and in their use of social media.
- they adhere to the Trust's E-security policy, with regard to the use of devices, systems and passwords and have an understanding of basic cybersecurity
- they have a general understanding of how the learners in their care use digital technologies outside the Trust, in order to be aware of online safety issues that may develop from the use of those technologies
- they are aware of the benefits and risks of the use of Artificial Intelligence (AI) services in Trust, being transparent in how they use these services, prioritising human oversight. AI should assist, not replace, human decision-making. Staff must ensure that final judgments, particularly those affecting people, are made by humans, fact-checked and critically evaluated.

IT Team

The IT Team is responsible for ensuring that:

- they are aware of and follow the Trust Online Safety Policy and E-Security Policy to carry out their work effectively in line with Trust policy
- the Trust technical infrastructure is secure and is not open to misuse or malicious attack
- the Trust meets (as a minimum) the required online safety technical requirements as identified by the DfE Meeting Digital and Technology Standards in Trusts & Colleges and guidance from local authority / MAT 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 Safeguarding Team and Head of Estates & IT for investigation and action
- the filtering policy is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person.
- monitoring systems are implemented and regularly updated as agreed in Trust policies

Learners

- are responsible for using the Trust digital technology systems in accordance with the learner acceptable use agreement 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.
- Learners will be supported to critically evaluate online information and recognise misinformation, disinformation, conspiracy theories, manipulative online content, deepfakes and AI-generated content. Online safety education will include developing critical thinking skills, digital literacy and resilience to online manipulation.
- should avoid plagiarism and uphold copyright regulations, taking care when using Artificial Intelligence (AI) services to protect the intellectual property of themselves and others and checking the accuracy of content accessed through AI services.
- should understand the importance of adopting good online safety practice when using digital technologies outside the Trust and realise that the Trust's Online Safety Policy covers their actions out of Trust, if related to their membership of the Trust.

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.

The Trust will take every opportunity to help parents and carers understand these issues through:

- publishing the Trust Online Safety Policy on the Trust website
- publish information about appropriate use of social media relating to posts concerning the Trust.
- 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 Trust in:

- reinforcing the online safety messages provided to learners in Trust.
- the safe and responsible use of their children's personal devices in the Trust (where this is allowed)

Professional Standards

There is an expectation that professional standards will be applied to online safety as in other aspects of Trust life i.e.

- there is a consistent emphasis on the central importance of literacy, numeracy, digital competence and digital resilience. Learners will be supported in gaining skills across

all areas of the curriculum and every opportunity will be taken to extend learners' skills and competence

- there is a willingness to develop and apply new techniques to suit the purposes of intended learning in a structured and considered approach and to learn from the experience, while taking care to avoid risks that may be attached to the adoption of developing technologies e.g. Artificial Intelligence (AI) tools.
- Staff are able to reflect on their practice, individually and collectively, against agreed standards of effective practice and affirm and celebrate their successes
- policies and protocols are in place for the use of online communication technology between the staff and other members of the Trust and wider community, using officially sanctioned Trust mechanisms.
- Where Generative AI is used to monitor staff communications, it will be balanced with respect for privacy and transparency about what is being monitored and why.

Acceptable use

The Trust has defined what it regards as acceptable/unacceptable use and this is shown in the tables below.

Acceptable use agreements

An Acceptable Use Agreement is a document that outlines a Trust's expectations on the responsible use of technology by its users. In most Trusts they are signed or acknowledged by their staff as part of their conditions of employment. Some may also require learners and parents/carers to sign them, though it is more important for these to be regularly promoted, understood and followed rather than just signed.

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated	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,	**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					**X**

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated	Unacceptable	Unacceptable and illegal
remarks, proposals or comments that contain or relate to:	• Public order offences - harassment and stalking • Drug-related offences • Weapons / firearms offences • Fraud and financial crime including money laundering N.B. Trusts should refer to current UKCIS guidance on "Sharing nudes and semi-nudes: advice for education settings working with children and young people".https://swgfl.org.uk/assets/documents/managing-sexting-incidents.pdf?_=1554476329https://www.gov.uk/government/publications/sexting-in-schools-and-colleges					
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 Trust 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	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 Trust policies:	Accessing inappropriate material/activities online in a Trust setting including pornography, gambling, drugs. (Informed by the Trust's filtering practices and/or AUAs)			X	X	
	Promotion of any kind of discrimination				X	
	Using Trust 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 Trust				X	
	Infringing copyright and intellectual property (including through the use of AI services)					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 Trust or brings the Trust into disrepute				X	

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

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

- users should immediately report to the DSL – in accordance with the Trust 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., Trust website and social media. Only Trust e-mail addresses should be used to identify members of staff and learners.

Reporting and responding

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

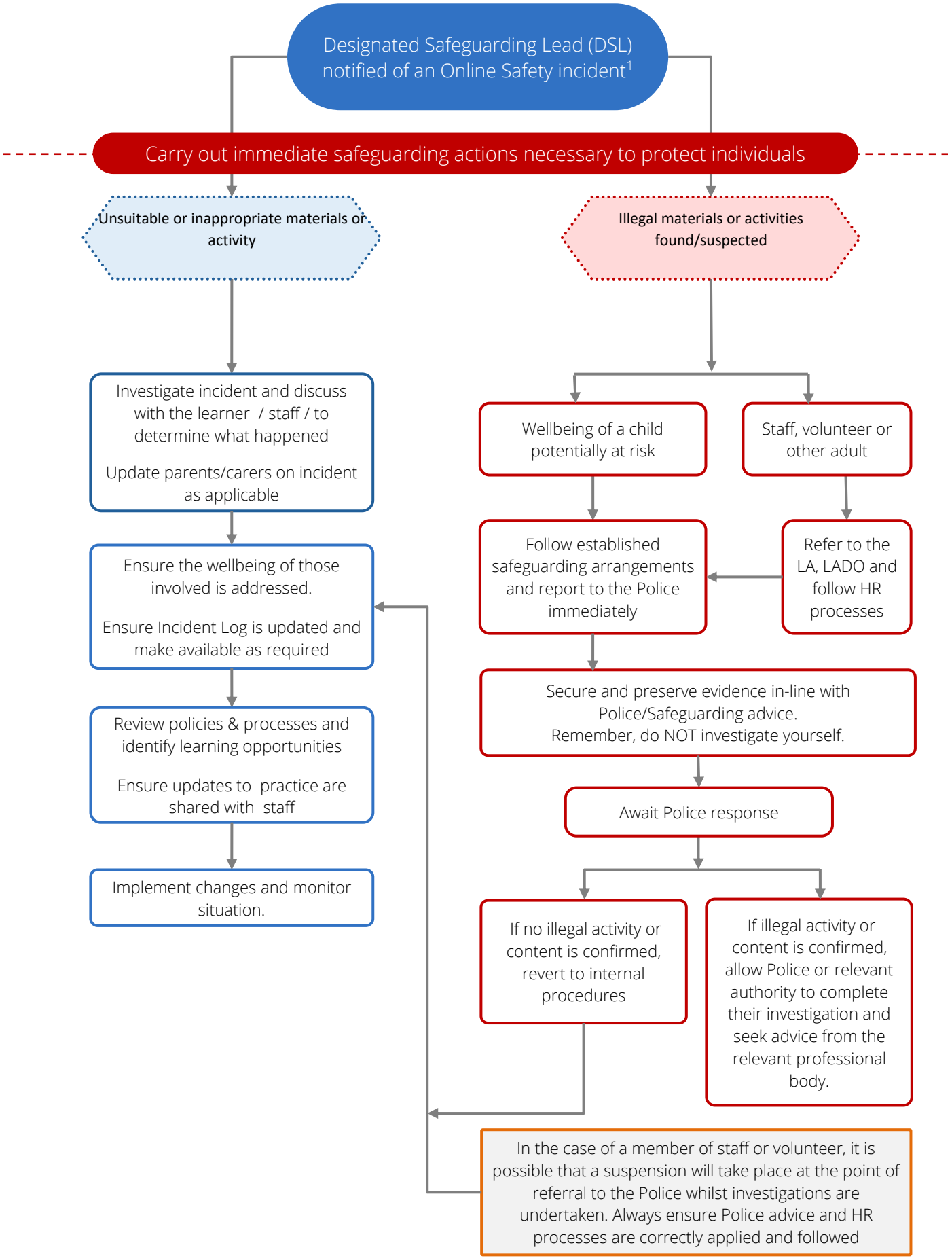
> *"Trust and college leaders should create a culture where sexual harassment and online sexual abuse are not tolerated, and where they identify issues and intervene early to better protect children and young people. ..In order to do this, they should assume that sexual harassment and online sexual abuse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

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

- there are clear reporting routes which are understood and followed by all members of the Trust community which are consistent with the Trust safeguarding procedures, and with the whistleblowing, complaints and managing allegations policies.
- all members of the Trust community will be made aware of the need to report online safety issues/incidents
- reports will be dealt with as soon as is practically possible once they are received
- the Designated Safeguarding Lead, or 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 the incident must be escalated through the agreed Trust safeguarding procedures, this may include
    - Non-consensual images
    - Self-generated images
    - Terrorism/extremism
    - Hate crime/ Abuse
    - Fraud and extortion
    - Harassment/stalking
    - Child Sexual Abuse Material (CSAM)

    - Child Sexual Exploitation Grooming
    - Extreme Pornography
    - Sale of illegal materials/substances
    - Cyber or hacking offences under the Computer Misuse Act
    - Copyright theft or piracy
- any concern about staff misuse will be reported to the Principal, unless the concern involves the Principal, in which case the complaint is referred to the CEO.
- where AI is used to support monitoring and incident reporting, human oversight is maintained to interpret nuances and context that AI might miss
- it is important that those reporting an online safety incident have confidence that the report will be treated seriously and dealt with effectively
- there are support strategies in place e.g., peer support for those reporting or affected by an online safety incident
- incidents should be logged.
- relevant staff are aware of external sources of support and guidance in dealing with online safety issues, e.g. local authority; police; Professionals Online Safety Helpline; Reporting Harmful Content; CEOP.
- 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, Trust social media, website
    - Trustees, through regular safeguarding updates
    - local authority/external agencies, as relevant (The Ofsted Review into Sexual Abuse in Trusts and Colleges suggested “working closely with Local Safeguarding Partnerships in the area where the Trust 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 Trust will make the flowchart below available to staff to support the decision-making process for dealing with online safety incidents.


Designated Safeguarding Lead (DSL) notified of an Online Safety incident[1]
Carry out immediate safeguarding actions necessary to protect individuals
Unsuitable or inappropriate materials or activity
Illegal materials or activities found/suspected
Investigate incident and discuss with the learner / staff / to determine what happened
Update parents/carers on incident as applicable
Ensure the wellbeing of those involved is addressed.
Ensure Incident Log is updated and make available as required
Review policies & processes and identify learning opportunities
Ensure updates to practice are shared with staff
Implement changes and monitor situation.
Wellbeing of a child potentially at risk
Staff, volunteer or other adult
Follow established safeguarding arrangements and report to the Police immediately
Refer to the LA, LADO and follow HR processes
Secure and preserve evidence in-line with Police/Safeguarding advice.
Remember, do NOT investigate yourself.
Await Police response
If no illegal activity or content is confirmed, revert to internal procedures
If illegal activity or content is confirmed, allow Police or relevant authority to complete their investigation and seek advice from the relevant professional body.
In the case of a member of staff or volunteer, it is possible that a suspension will take place at the point of referral to the Police whilst investigations are undertaken. Always ensure Police advice and HR processes are correctly applied and followed

Trust actions

It is more likely that the Trust will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the Trust community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary policies. The Trust recognises that many online safeguarding concerns occur outside the academy environment and outside academy hours. Where such concerns affect a child's welfare, safety, wellbeing or ability to access education, the Trust will take appropriate safeguarding action in accordance with the Child Protection Policy.

The use of Artificial Intelligence (AI) systems in the Trust

As Generative Artificial Intelligence (gen AI) continues to advance and influence the world we live in, its role in education is also evolving. There are currently 3 key dimensions of AI use in Trusts: learner support, teacher support and Trust operations; ensuring all use is safe, ethical and responsible is essential.

We realise that there are risks involved in the use of Gen AI services, but that these can be mitigated through our existing policies and procedures, amending these as necessary to address the risks.

We will educate staff and learners about safe and ethical use of AI, preparing them for a future in which these technologies are likely to play an increasing role.

The safeguarding of staff and learners will, as always, be at the forefront of our policy and practice.

The Trust recognises that AI technologies may create safeguarding risks including AI-generated sexual images, deepfakes, impersonation, AI-enabled bullying, grooming through AI chatbots, online scams, inaccurate AI information and the dissemination of harmful or extremist content.

For more information on the use of AI within the Trust, please refer to the Trust AI Policy.

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 Trust 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: (select/delete as appropriate)

- a planned programme of formal online safety and data protection training will be made available to all staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.
- the training will be an integral part of the Trust's annual safeguarding, data protection and cyber-security training for all staff
- Online safety training is integrated within safeguarding training and reflects emerging safeguarding risks including child-on-child abuse, harmful sexual behaviour, online sexual abuse, misinformation, disinformation, radicalisation, AI-enabled harms and cyber-enabled exploitation.
- Each Academy Online safety lead and/or 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/Academy Online safety Lead (or other nominated person) will provide advice/guidance/training to individuals as required.
- All online safety concerns will be recorded on the Trust safeguarding recording system in accordance with the Trust Child Protection Policy. Records will include actions taken, outcomes achieved and any referrals made to external agencies.

Families

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring/ regulation of the children's online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The Trust 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
- 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).

Student Voice

Horizons Specialist Academy Trust recognises the crucial role that learner voice plays in developing effective, relevant and inclusive online safety practice. Learners should feel empowered to share their experiences, express concerns, contribute ideas and influence how the Trust approaches online safety.

The Trust is committed to ensuring that all learners — including those with SEND and communication differences — have meaningful, accessible opportunities to participate in shaping online safety provision.

To achieve this, the Trust will:

- **Seek learner feedback regularly** through surveys, discussion groups, school council forums, and informal conversations, ensuring materials are adapted appropriately for learners with communication needs.
- **Include learner representatives** (where appropriate) in reviewing online safety education, reporting routes and acceptable use expectations, ensuring they reflect the lived experiences and needs of our learners.
- **Use learner voice** to inform curriculum planning, resource development and online safety campaigns, including events such as Safer Internet Day, Anti-Bullying Week and digital resilience initiatives.
- **Ensure accessible reporting routes** so learners can safely report concerns, ask questions or request support. This may include visual systems, trusted adults, worry boxes, communication aids or digital tools.
- **Promote a culture where learner concerns are listened to, taken seriously and acted upon**, with outcomes fed back in an appropriate and accessible way.
- **Support learners to become positive digital role models**, celebrating their contributions, achievements and leadership in promoting safe, respectful and responsible online behaviour.
- **Ensure learners understand their rights and responsibilities online**, including how their voice helps improve online safety for themselves and others across the Trust.

Through embedding student voice at all levels, the Trust will develop a more responsive, relevant and inclusive approach to online safety that reflects the experiences and needs of the children and young people we serve.

Technology

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

The Trust is responsible for ensuring that the Trust infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. The Trust should ensure that all staff are made aware of policies and

procedures in place on a regular basis and explain that everyone is responsible for online safety and data protection.

Filtering & Monitoring

The DfE guidance (for England) on filtering and monitoring in "Keeping Children Safe in Education" 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 Trust's or college's IT system. As part of this process, governing bodies and proprietors should ensure their Trust 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 Trusts and colleges and will be informed in part, by the risk assessment required by the Prevent Duty. To support Trusts and colleges to meet this duty, the Department for Education has published filtering and monitoring standards…"

The Trust filtering and monitoring provision is agreed by senior leaders, Trustees and the IT Team 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 with support from the Trust safeguarding team will have lead responsibility for safeguarding and online safety and the IT team will have technical responsibility.

The filtering and monitoring provision is reviewed (at least annually) by senior leaders, the Trust Safeguarding Team and a Trustee with the involvement of the Head of IT and Estates.

Checks on the filtering and monitoring system are carried out by the IT team with the involvement of a senior leader, the Trust safeguarding team and a Trustee.

The Trust Safeguarding Team, Head of Estates & IT and safeguarding Trustee will receive regular filtering and monitoring assurance reports throughout the academic year. These reports will be reviewed alongside safeguarding trends to ensure systems remain effective and proportionate to identified risks.

Filtering

The DfE Technical Standards for Trusts and Colleges states:

"Trusts and colleges have a statutory responsibility to keep children and young people safe online as well as offline. Governing bodies and proprietors should make sure their Trust or college has appropriate filtering and monitoring systems in place, as detailed in the statutory guidance, Keeping children safe in education.

Filtering is preventative. It refers to solutions that protect users from accessing illegal, inappropriate and potentially harmful content online. It does this by identifying and blocking specific web links and web content in the form of text, images, audio and video

These standards help Trust and college leaders, designated safeguarding leads and IT support understand how to work together to make sure they can effectively safeguard their students and staff."

- 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. These are acted upon in a timely manner, within clearly established procedures
- there is a clear process in place to deal with, and log, requests/approvals for filtering changes
- filtering logs are regularly reviewed and alert the Trust Safeguarding Team to breaches of the filtering policy.
- There are regular checks of the effectiveness of the filtering systems. The Trust Safeguarding Team and Trustee are involved in the process and aware of the findings.

Monitoring

The DfE Technical Standards for Trusts and Colleges states:

"Monitoring is reactive. It refers to solutions that monitor what users are doing on devices and, in some cases, records this activity. Monitoring can be manual, for example, teachers viewing screens as they walk around a classroom. Technical monitoring solutions rely on software applied to a device that views a user's activity. Reports or alerts are generated based on illegal, inappropriate, or potentially harmful activities, including bullying. Monitoring solutions do not block users from seeing or doing anything."

The Trust has monitoring systems in place, agreed by senior leaders and technical staff, to protect the Trust, systems and users:
The Trust monitors all network use across all its devices and services.

- monitoring reports are urgently picked up, acted on, all users are aware that monitoring is in place.
- There are effective protocols in place to report abuse/misuse. There is a clear process for prioritising response to alerts that require rapid safeguarding intervention.

- Management of serious safeguarding alerts is consistent with safeguarding policy and practice.
- The monitoring provision is reviewed at least once every academic year and updated in response to changes in technology and patterns of online safety incidents and behaviours. The review is be conducted by members of the senior leadership team, the Trust safeguarding Team, and technical staff. It will also involve the responsible Trustee. The results of the review will be recorded and reported as relevant.
- monitoring enables alerts to be matched to users and devices.

Managing the use of Mobile Phones, Smart Watches and other devices

Mobile phones and smart watches are considered to be an everyday item in today's society. They can be used in a variety of ways to communicate through texting, photography and internet accesses.
However, mobile phones and smart watches can present a number of problems when not used appropriately:

- They are valuable items which may be stolen or damaged.
- Their use can render students or staff subject to cyberbullying.
- Internet access on phones and personal devices can allow students to bypass security settings and filtering.
- They can undermine classroom discipline as they can be used on silent mode.
- Mobile phones with integrated cameras could lead to child protection, bullying and data protection issues with regard to inappropriate capture, use or distribution of images of students or staff.

It is therefore the Trust's policy to advise that all children and young people under 16 leave their mobile phones and smart watches at home and the students who attend the 6th Form at Abbey Hill Academy hand them in at reception at the beginning of the day. Failure to comply with this rule will be dealt with through the Trust's Behaviour Policy (see Behaviour Policy).

- The sending of abusive or inappropriate messages or content via mobile phones and smart watches is forbidden by any member of the Trust community and any breaches will be dealt with via the Trust's Behaviour Policy.
- Staff's use of mobile phones and smart watches will not be permitted during any lesson with children and young people.
- Staff are not permitted to contact children, young people and families with their own personal mobile phone or smart watch.
- Staff must not use personal devices to communicate with pupils or families except where expressly authorised through Trust procedures. Staff must also follow the Staff Code of Conduct, Safer Working Practices and Child Protection Policy.
- Staff should not use personal mobile phones to take pictures or videos of students, if it is believed that this is the case disciplinary action may be taken.

Social Networking, Social Media and Personal Publishing

The internet has constantly evolving online spaces and social networks which allow individuals to publish unmediated content. Social networking sites can connect people with similar or very different interests. Users can be invited to view personal spaces and leave comments, over which there may be limited control.

Students and students will be encouraged through the curriculum to think about the ease of uploading personal information, the associated dangers and the difficulty in removing an inappropriate image or information once published.

Similarly, through Professional Learning all staff will be made aware of the potential risks in using social networking sites of personal publishing either professionally with students and students or personally. They will also be aware of the importance of considering the material they post, ensuring profiles are secured and how publishing unsuitable material may affect their professional status.

- Staff are not allowed to be "friends" with any children, young people or families they work with on social networking sites**.** (see HSAT Social Networking Guidance)
- The Trust will control access to social media and social networking sites whilst on site or using a Trust provided device.
- Students will be advised never to give out personal information which may identify them or their location.
- All social media and associated tools are currently banned however if staff wish to use social media tools with students and students as part of the curriculum they will need to risk assess the sites before use and check the sites terms and conditions to ensure the site is age appropriate. Permission will then need to be sought from the Principal of the Academy and a request made to the ICT Network Manager to allow access to a particular site.
- Students will be advised on security and privacy online and will be encouraged to set passwords, deny access to unknown individuals and to block unwanted communications.
- All members of the Trust community are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.
- Concerns regarding pupil and students use of social networking, media and personal publishing sites (in and out of school) will be raised with their parents or carers, particularly with the use of 18+ sites.
- Staff personal use of social networking, social media and personal publishing sites will be discussed as part of staff induction and safe and professional behaviour will be outlined in the Trust's Acceptable use Agreement.

Sharing Nudes and Semi-Nudes: Responding to incidents and safeguarding children and young people

This section covers the sharing of nudes and semi-nudes by children and young people. The term "sharing nudes and semi-nudes" means the sending or posting of nude or semi-

nude images, videos or live streams by young people under the age of 18. Creating, possessing or sharing nude or semi-nude images of anyone under 18 may constitute an offence; incidents will be managed proportionately as safeguarding concerns in line with current UKCIS guidance.

Although the production of such imagery described above is likely to take place outside of an academy, the issues that follow on from this are likely to manifest themselves in our academies therefore we need to be able to respond swiftly and confidently to ensure that children and young people are safeguarded, supported and educated.

The guidance supports academies in developing procedures to respond to incidents involving the sharing of nudes and semi-nudes and signposts to relevant resources and support.

The procedures outlined in the guidance should form part of the Trust's Child Protection arrangements and all incidents involving the sharing of nudes and semi-nudes should be dealt with as safeguarding concerns.

Sexual harassment, online sexual abuse, sexual violence

The Trust recognises that online abuse between children can include cyberbullying, sexual harassment, sexual violence, image-based abuse, coercive behaviour, exploitation, harmful sexual behaviour and discriminatory abuse. Such incidents will be managed as safeguarding concerns and not solely as behaviour matters.

Sexual violence and sexual harassment can occur between two children of any age and sex from primary through to secondary stage and into colleges. It can occur through a group of children sexually assaulting or sexually harassing a single child or group of children. Sexual violence and sexual harassment exist on a continuum and may overlap; they can occur online and face to face (both physically and verbally) and are never acceptable. As set out in Part one of Keeping children safe in education (KCSIE), all staff working with children are advised to maintain an attitude of 'it could happen here'. Any incidents of online sexual abuse will be dealt with in accordance to the Trust's Child Protection Policy and Part 5 of Keeping Children Safe in Education.

Child-on-child abuse may also include image-based abuse, coercive behaviour, online exploitation by peers, group-based online abuse and harmful sexual behaviour online. Such behaviour will be treated as a safeguarding concern and addressed in line with the Trust's Child Protection Policy.

Resources and support

- In addition to Local Safeguarding Partner resources, advice can be found in "Sharing nudes and semi-nudes: advice for education settings working with children and young people": https://www.gov.uk/government/publications/sharing-nudes-and-semi-nudes-

advice-for-education-settings-working-with-children-and-young-peoplehttps://www.gov.uk/government/publications/sexting-in-schools-and-colleges

The following resources can be used to support parents and carers and children and young people with youth produced sexual imagery:

Helplines and reporting

- Children and young people can talk to a ChildLine counsellor 24 hours a day about anything that is worrying them by ringing 0800 11 11 or in an online chat at http://www.childline.org.uk/Talk/Chat/Pages/OnlineChat.aspx
- If parents or carers are concerned that their child or young person is being contacted by adults as a result of having shared sexual imagery they should report to NCA-CEOP at https://www.ceop.police.uk/safety-centre/
- ChildLine and the Internet Watch Foundation have partnered to help children and young people get sexual or naked images removed from the internet. More information is available at http://www.childline.org.uk/explore/onlinesafety/ pages/sexting.aspx
- If parents and carers are concerned about their child or young person, they can contact the NSPCC Helpline by ringing 0808 800 5000, by emailing help@nspcc.org.uk, or by texting 88858. They can also ring the Online Safety Helpline by ringing 0808 800 5002.

Advice and information for parents and carers

- The NSPCC has information and advice about sharing nudes and semi-nudes available on its website: https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/sexting/1
- NCA-CEOP has produced a film resource for parents and carers to help them prevent their children coming to harm through sharing sexual imagery: https://www.ceopeducation.co.uk/parents/articles/Nude-selfies-a-parents-guide/.
- Childnet have information and advice about sharing nudes and semi-nudes available on its website: https://www.childnet.com/help-and-advice/sexting/

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. It is common for employers to carry out internet searches for information about potential and existing employees.

The Trust will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- the Trust may use live-streaming or video-conferencing services in line with national and local safeguarding guidance / policies.
- 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/volunteers must be aware of those learners whose images must not be taken/published. Those images should only be taken on Trust devices. The personal devices of staff should not be used for such purposes
- staff and volunteers are allowed to take digital/video images to support educational aims, but must follow Trust policies 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.
- images will be securely stored in line with the Trust retention policy

Online Publishing

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

- Public-facing website
- Social media
- Online newsletters

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

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

<u>The DfE Cyber security standards for Trusts and colleges explains:</u>

> "Cyber incidents and attacks have significant operational and financial impacts on Trusts and colleges. These incidents or attacks will often be an intentional and unauthorised attempt to access, change or damage data and digital technology. They could be made by a person, group, or organisation outside or inside the Trust or college and can lead to:

- safeguarding issues due to sensitive personal data being compromised
- impact on student outcomes
- a significant data breach
- significant and lasting disruption, including the risk of repeated future cyber incidents and attacks, including Trust or college closure
- financial loss
- reputational damage"

The 'Cyber-security in Trusts: questions for governing bodies and Trustees' guidance produced by the National Cyber Security Centre (NCSC) aims to support governing bodies' and management committees' understanding of their education settings' cyber security risks. The guidance includes eight questions to facilitate the cyber security conversation between the governing body and Trust leaders, with the governing body taking the lead.

The Trust may wish to consider the following statements, amending them in the light of their current cybersecurity policy, processes and procedures:

- the Trust has reviewed the DfE Cyber security standards for Trusts and colleges and is working toward meeting these standards
- the Trust, has identified the most critical parts of the Trust's digital and technology services and sought assurance about their cyber security
- the Trust has an effective backup and restoration plan in place in the event of cyber attacks
- the Trust's governance and IT policies reflect the importance of good cyber security
- staff and Governors receive training on the common cyber security threats and incidents that Trusts experience
- the Trust's education programmes include cyber awareness for learners
- the Trust has a business continuity and incident management plan in place
- there are processes in place for the reporting of cyber incidents. All students and staff have a responsibility to report cyber risk or a potential incident or attack, understand how to do this feel safe and comfortable to do so.
- Cyber incidents which may create safeguarding risks will be reported immediately to the Designated Safeguarding Lead and IT Team.

Prevent Duty

Horizons Specialist Academy Trust recognises its duty under the Counter-Terrorism and Security Act 2015 to have due regard to the need to prevent people from being drawn into terrorism. The Trust is committed to safeguarding all learners, staff and the wider community from the risks of radicalisation, extremism, and extremist ideology.

As a Specialist Academy Trust, we understand that some of our learners may be more vulnerable to radicalisation due to their additional needs, social circumstances or online influences. We therefore ensure that the Prevent Duty is embedded within our safeguarding, curriculum and online safety practices.

Our Approach:

- **Leadership and Governance:** The Nominated Trustee and Trust Designated Safeguarding Lead (DSL) are responsible for ensuring compliance with the Prevent Duty across the Trust. All academies have clear procedures for identifying and responding to concerns related to radicalisation or extremism. The Trust's safeguarding trustee receive regular updates on Prevent activity and training.
- **Training and Awareness:** All staff receive Prevent awareness training as part of their safeguarding induction and ongoing CPD. This ensures that they can identify early signs of radicalisation, challenge extremist views safely, and know how to refer concerns using the Trust's safeguarding procedures.
- **Curriculum:** The Trust promotes British Values — democracy, rule of law, individual liberty, and mutual respect and tolerance for those with different faiths and beliefs — through its curriculum, assemblies and wider personal development programmes. Learners are supported to develop digital literacy and critical thinking skills to challenge extremist narratives online.
- **Partnership Working:** The Trust works closely with local safeguarding partners, the Police Prevent Team, local authorities, and Channel Panels where appropriate.
- **Online Safety:** Online safety education includes awareness of extremist and radicalising content. The Trust's filtering and monitoring systems are used to identify and block extremist material and report any attempts to access such content.
- **Referral Procedures:** Concerns that a child, young person or member of staff may be vulnerable to radicalisation are treated as safeguarding matters and reported to the DSL, who will assess the concern and make referrals to the Local Authority Prevent or Channel Panel as appropriate.

Through this approach, Horizons Specialist Academy Trust seeks to create a safe, inclusive and resilient community where all learners can thrive, free from the risks of extremism and radicalisation.