Online Safety Policy

Contents

1. Aims

Our Trust aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and Directors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole Trust community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scam

2. Legislation and guidance

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

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

This policy complies with our funding agreement and articles of association.

3. Roles and responsibilities

3.1 The Board of Directors

The Board of Directors has overall responsibility for monitoring this policy and holding others to account for its implementation.

The Board of Directors will co-ordinate regular meetings with appropriate staff to discuss online safety.

It is essential that the Board of Directors ensure that appropriate filtering and monitoring systems are in place across the whole organisation and regularly review their effectiveness. The Directors should be doing all that they reasonably can to limit children's exposure to the risks from the academy's IT system.

The Board of Directors will ensure that the leadership team and relevant staff have an awareness and understanding of the filtering and monitoring provisions in place and manage them effectively and know how to escalate concerns when identified. A review report must be seen annually.

The Board of Directors will review the standards set out in the DfE published filtering and monitoring guidance and discuss with IT staff and service providers what more needs to be done to support the organisation to meet these.

The Director who oversees online safety is expected to:

- Hold regular meetings with the DSP/Online Safety Co-ordinator for each setting
- Ensure attendance at Online Safety Group meetings, which are incorporated into the Trust Safeguarding meeting
- Complete regular monitoring of online safety incident logs provided by the designated safeguarding person (DSP) and Online Safety Lead (where different from the DSP)
- Complete regular monitoring of the effectiveness of filtering/change control logs.

All Directors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the Trust's ICT systems and the internet (Appendix 3)
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with SEND because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

3.2 The Principal

The Principal is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the academy. This includes:

- appointing an Online Safety Lead;

- ensuring the safety (including online safety) of members of the academy community, though the day to day responsibility for online safety will be delegated to the DSP/Online Safety Lead (If different);
- being aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. (see flow chart on dealing with online safety incidents);
- ensuring that the Online Safety Lead and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant;
- ensuring there is an effective system in place in the academy to filter contents open to pupils and staff and a system which monitors the IT work of pupils and staff;
- ensuring that online safety and details of the Trust filtering and monitoring systems are included as part of regular training for all staff and as part of the induction training for all new staff;
- ensuring that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles;
- receiving regular monitoring reports from the Online Safety Lead.

3.3 The DSP and Online Safety Lead

Details of each academy DSP and deputies are set out in the HAT Child Protection Policy as well as relevant job descriptions.

The DSP takes lead responsibility for online safety in each academy but may delegate the role of Online Safety Lead where agreed with the Principal. The DSP will:

- support the Principal in ensuring that staff understand this policy and that it is being implemented consistently throughout the academy;
- work with the Principal, IT Manager and other staff, as necessary, to address any online safety issues or incidents
- manage all online safety issues and incidents in line with the Trust's policies;
- ensuring that any incidents of cyber-bullying are dealt with appropriately in line with each academy behaviour policy
- ensure that any online safety incidents are logged (see Appendix 5) and dealt with appropriately in line with this policy, including those picked up by the IT monitoring system;
- ensure that any incidents of cyber-bullying are logged and dealt with appropriately in line with the academy behaviour policy;
- update and deliver staff training on online safety (Appendix 4 contains a self-audit for staff on online safety training needs);
- liaise with other agencies and external services if necessary;
- provide regular reports on online safety to the Principal, Director of Finance and Operations, Chief Executive Officer or Board of Directors as required.

This list is not intended to be exhaustive.

3.4 The IT Manager

The IT Manager is responsible for:

- putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at the academy, including terrorist and extremist material;
- ensuring that the Trust's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly;
- conducting a full security check and monitoring the Trust's ICT systems on a weekly basis;
- blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files;
- ensuring that all users may only access the networks and devices through a properly enforced password protection policy;
- ensuring that any online safety incidents are logged (see Appendix 5) and dealt with appropriately in line with this policy.

This list is not intended to be exhaustive.

3.5 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- maintaining an understanding of this policy;
- maintaining an understanding of the Trust's filtering and monitoring system and their responsibilities in implementing it;
- implementing this policy consistently;
- agreeing and adhering to the terms on acceptable use of the Trust's ICT systems and the internet (Appendix 3), and ensuring that pupils follow the Trust's terms on acceptable use (Appendices 1 and 2);
- working with the DSL to ensure that any online safety incidents are logged (see Appendix 5) and dealt with appropriately in line with this policy;
- ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the academy behaviour policy;
- ensuring pupils understand and follow the Online Safety Policy and acceptable use policies;
- ensuring pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations;
- checking all internet sites that are planned to be used as suitable and that processes are in place for dealing with any unsuitable material that is found in internet searches;
- responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'.

This list is not intended to be exhaustive.

3.6 Parents/Carers

Parents/carers are expected to:

- notify a member of staff or the Principal of any concerns or queries regarding this policy;
- ensure their child has read, understood and agreed to the terms on acceptable use of the Trust's ICT systems and internet (Appendices 1 and 2);

Parents/carers can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? – UK Safer Internet Centre
- Hot topics – Childnet International
- Parent resource sheet – Childnet International
- Healthy relationships – Disrespect Nobody

3.7 Visitors and members of the community

Visitors and members of the community who use the Trust's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (Appendix 3).

3.8 Pupils

Pupils are expected to:

- be responsible for using the academy network and digital technology systems in accordance with the acceptable use agreement;
- understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so;
- know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking/use of images and on online-bullying;
- understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the academy's online safety policy covers their actions out of school, if related to their membership of the school;
- where appropriate, have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.

4. Educating pupils about online safety

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

Reference must be made to the DfE's **Teaching online safety in schools** as a ready source of guidance to support the effective teaching of online safety for all pupils. Online Safety Leads in each academy should support staff with referencing this document.

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression.

All Trust academies have to teach:

- Relationships education and health education in primary academies
- Relationships and sex education and health education in secondary academies

Trust primary academies

In **Key Stage 1**, pupils will be taught to:

- use technology safely and respectfully, keeping personal information private;
- identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies.

Pupils in **Key Stage 2** will be taught to:

- use technology safely, respectfully and responsibly;
- recognise acceptable and unacceptable behaviour;
- identify a range of ways to report concerns about content and contact.

By the **end of primary**, pupils will know:

- that people sometimes behave differently online, including by pretending to be someone they are not;
- that the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous;
- the rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them;
- how to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met;
- how information and data is shared and used online;
- what sorts of boundaries are appropriate in friendships with peers and others (including in a digital context);
- how to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know.

Trust secondary academies

In **Key Stage 3**, pupils will be taught to:

- understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy;
- recognise inappropriate content, contact and conduct, and know how to report concerns.

Pupils in **Key Stage 4** will be taught:

- to understand how changes in technology affect safety, including new ways to protect their online privacy and identity;
- how to report a range of concerns.

By the **end of secondary**, pupils will know:

- their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online;
- about online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online;
- not to provide material to others that they would not want shared further and not to share personal material which is sent to them;
- what to do and where to get support to report material or manage issues online;
- the impact of viewing harmful content;
- that specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners;
- that sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties including jail;
- how information and data is generated, collected, shared and used online;
- how to acknowledge the source of information used and to respect copyright when using material accessed on the internet;
- how to build resilience to radicalisation by providing a safe environment for debating issues, including those which could be seen as controversial, and helping them to understand how they can influence and participate in decision-making;
- how to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours;
- how people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online.

The safe use of social media and the internet will also be covered in other subjects where relevant.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

5. Educating parents/carers and the wider community about online safety

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

- curriculum activities;
- letters, newsletters, web site, apps, Learning Platform;
- parents/carers information sessions;

- high profile events e.g. Safer Internet Day;
- their websites will provide online safety information for the wider community;
- sharing their online safety expertise/good practice with other local schools;
- supporting community groups e.g. Early Years Settings, Childminders, youth/sports/voluntary groups to enhance their online safety provision as requested.

This policy will also be shared with parents/carers.

If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the Principal and/or the DSP.

Concerns or queries about this policy can be raised with any member of staff or the Principal.

6. Cyber-bullying

6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. See HAT Anti Bullying Policy.

6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

Each academy will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, Directors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

Each academy also sends information on cyber-bullying to parents/carers so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the academy will follow the processes set out in the Trust's Anti-Bullying Policy and each academy behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the academy will use all reasonable endeavours to ensure the incident is contained.

The DSP will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices

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

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

- cause harm;
- disrupt teaching;
- break any of the academy rules.

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

- delete that material;
- retain it as evidence (of a criminal offence or a breach of discipline);
- report it to the police*.

* Staff may also confiscate devices for evidence to hand to the police, if a pupil discloses that they are being abused and that this abuse includes an online element.

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on screening, searching and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- The Trust's COVID-19 risk assessment

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

7. Acceptable use agreement

All pupils, parents/carers, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the Trust's ICT systems and the internet (Appendices 1-3). Visitors will be expected to read and agree to the Trust's terms on acceptable use if relevant.

Use of the Trust's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, directors and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements in Appendices 1, 2 and 3.

8. Pupils using mobile devices in school

Pupils who attend a secondary academy or key stage 2 in a primary academy may bring mobile devices in, but are not permitted to use them during the school day. In primary

academies they must be handed to academy staff at the start of the day and in secondary academies they must be turned off and kept out of view in a bag during the day.

Sixth Form pupils may use their mobile device for study purposes only in designated academy areas.

Any use of mobile devices in each academy by pupils must be in line with each academy behaviour policy and the acceptable use agreement (see appendices 1 and 2).

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the academy behaviour policy, which may result in the confiscation of their device.

9. Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol);
- using multi-factor authentication as required;
- ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device;
- not using an external hard drive to store files for work related purposes;
- making sure the device locks if left inactive for a period of time;
- not sharing the device among family or friends;
- updating security software as prompted by the IT Team;
- keeping operating systems up to date – always install the latest updates.

Staff members must not use the device in any way which would violate the Trust's terms of acceptable use, as set out in Appendix 3.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from the IT Team or Principal. The must follow the steps set out in the Trust's Cyber Security Protocol.

10. Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for 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 academy will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular, they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.

Written permission from parents or carers will be obtained before photographs of pupils are published on the academy website/social media accounts/local press. Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images. Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.

Pupils must not take, use, share, publish or distribute images of others without their permission.

Pupil's work can only be published with the permission of the pupil and parents or carers.

In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at the academy events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other pupils in the digital/video images.

Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow academy policies concerning the sharing, distribution and publication of those images. Those images should only be taken on academy equipment; the personal equipment of staff must not be used for such purposes.

Care should be taken when taking digital/video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the academy into disrepute.

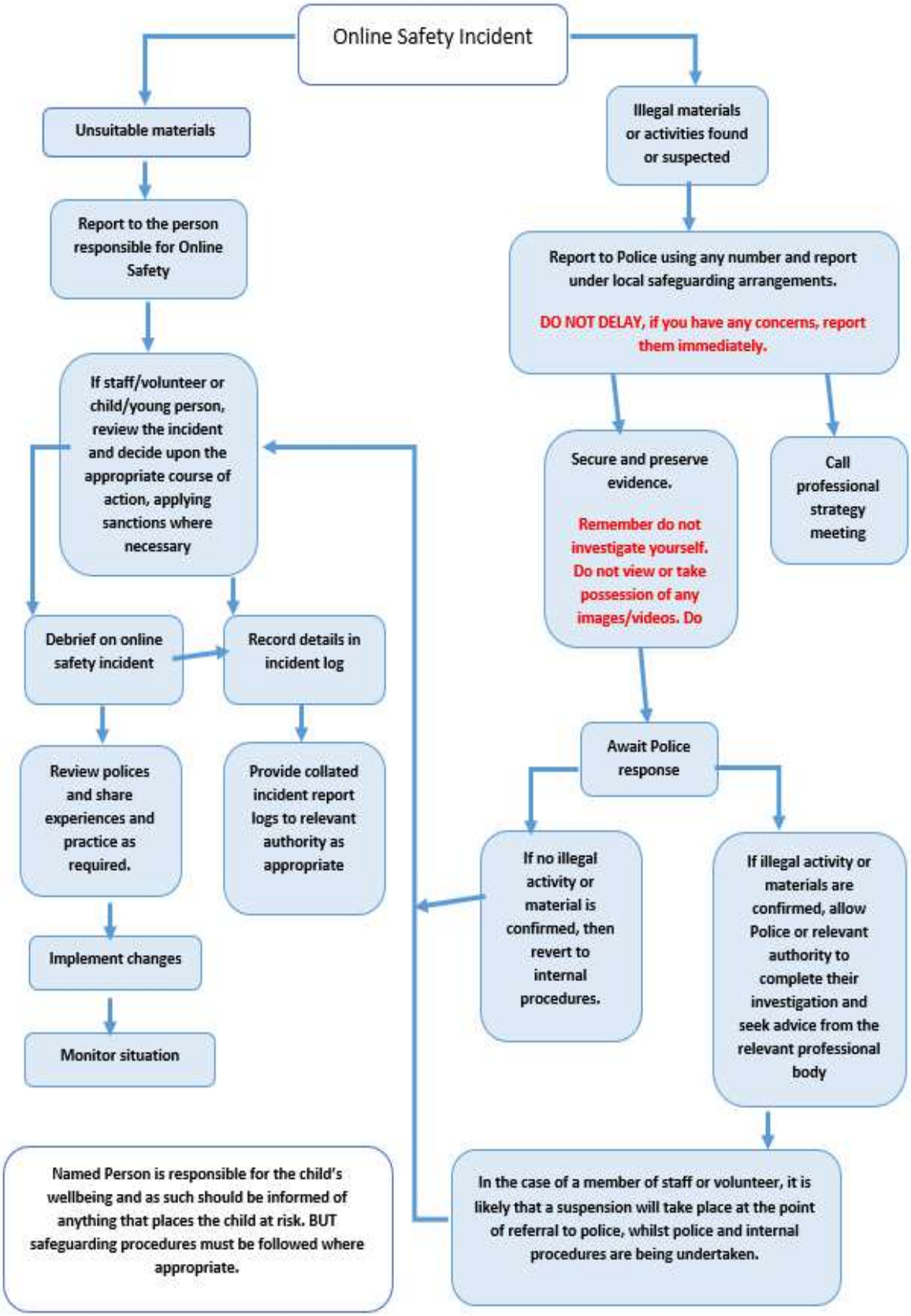
11. How the Trust will respond to issues of misuse

Where a pupil misuses the Trust's ICT systems or internet, we will follow the procedures set out in our academy behaviour policies. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the Trust's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the Trust's disciplinary policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The Trust will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

The flow chart below will be used to determine the most appropriate next step:


Online Safety Incident
Unsuitable materials
Illegal materials or activities found or suspected
Report to the person responsible for Online Safety
Report to Police using any number and report under local safeguarding arrangements.
DO NOT DELAY, if you have any concerns, report them immediately.
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Secure and preserve evidence.
Remember do not investigate yourself. Do not view or take possession of any images/videos. Do
Call professional strategy meeting
Debrief on online safety incident
Record details in incident log
Review polices and share experiences and practice as required.
Provide collated incident report logs to relevant authority as appropriate
Await Police response
Implement changes
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
Monitor situation
Named Person is responsible for the child's wellbeing and as such should be informed of anything that places the child at risk. BUT safeguarding procedures must be followed where appropriate.
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.

12. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber security, cyber bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required. This training will be organised and provided by the DSP (or Online Safety Lead if different).

All staff will receive update training or details regarding the Trust's filtering and monitoring systems being used.

The Trust expects all staff members and Directors will complete the National College CPD entitled – Annual Certificate in Online Safety and the NCSC - Cyber Security training for school staff.

By way of these training opportunities, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
    - Abusive, harassing, and misogynistic messages
    - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
    - Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- develop better awareness to assist in spotting the signs and symptoms of online abuse
- develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh the risks up
- develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSP (and Deputy DSLs) will undertake child protection training, which will include online safety, at least every year. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Volunteers will receive appropriate training and updates, if applicable.

Training requirements will will be regularly updated and reinforced as new guidance is produced or in response to an online safety incident.

13. Monitoring arrangements

The DSP logs behaviour and safeguarding issues related to online safety. An incident report log can be found in Appendix 5.

This policy will be reviewed every year by the CEO. At every review, the policy will be shared with the Board of Directors. The review (such as the one available here) will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

14. Links with other policies

This online safety policy is linked to:

- HAT Child Protection policy
- HAT Academy Behaviour policy
- HAT Cyber Security policy
- HAT Staff Code of Conduct
- HAT Data Protection policy and privacy notices
- HAT Complaints policy
- Acceptable use agreements

Appendix 1: EYFS and KS1 Acceptable Use Agreement (pupils and parents/carers)

ACCEPTABLE USE OF THE TRUST'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS	
Name of pupil:	

The Trust uses Smoothwall filtering and monitoring of all online activities by pupils. More details can be found here.
When I use the Trust's ICT systems (like computers) and get onto the internet in school I will:
• Ask a teacher or adult if I can do so before using them
• Only use websites that a teacher or adult has told me or allowed me to use
• Tell my teacher immediately if:
  o I click on a website by mistake
  o I receive messages from people I don't know
  o I find anything that may upset or harm me or my friends
• Use academy computers or devices for school work only
• Be kind to others and not upset or be rude to them
• Look after the ICT equipment and tell a teacher straight away if something is broken or not working properly
• Only use the username and password I have been given
• Try my hardest to remember my username and password
• Never share my password with anyone, including my friends.
• Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carer
• Save my work on the academy network
• Check with my teacher before I print anything
• Log off or shut down a computer when I have finished using it
I agree that the Trust will monitor the websites I visit and that there will be consequences if I don't follow the rules.	

Signed (pupil):	**Date:**
Parent/carer agreement: I agree that my child can use the Trust's ICT systems and internet when appropriately supervised by a member of academy staff. I agree to the conditions set out above for pupils using the Trust's ICT systems and internet, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Appendix 2: KS2, KS3, KS4 & KS5 Acceptable Use Agreement (pupils and parents/carers)

ACCEPTABLE USE OF THE TRUST'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS

Name of pupil:

The Trust uses Smoothwall filtering and monitoring of all online activities by pupils. More details can be found here.

I will read and follow the rules in the acceptable use agreement policy.

For my own personal safety:

- I understand that the academy will monitor my use of the systems, devices and digital communications.
- I will keep my username and password safe and secure – I will not share it, 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 be aware of "stranger danger", when I am communicating on-line.
- I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc.)
- If I arrange to meet people off-line that I have communicated with on-line, I will do so in a public place and take an adult with me.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

I understand that everyone has equal rights to use technology as a resource and:

- I understand that the Trust and academy systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission.
- 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 use the Trust and academy systems or devices for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (e.g. YouTube), unless I have permission of a member of staff to do so.

I will act as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.

When using the internet for research or recreation, I recognise that:

- I should 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 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 that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me
- I will only use artificial intelligence for academic work when instructed to by a member of staff and ensure that this is clearly referenced within the work itself.

ACCEPTABLE USE OF THE TRUST'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS

I recognise that the Trust and academy has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the academy:

- I will not use it during lessons, tutor group time, clubs or other activities organised by the academy, without a teacher's permission.
- I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online.
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I 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 immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person/organisation who sent the email, 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 not install or attempt to install or store programmes of any type on any academy device, nor will I try to alter computer settings.
- I will only use social media sites with permission and at the times that are allowed.

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

- I understand that the academy also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be online-bullying, use of images or personal information).
- I understand that if I fail to comply with this acceptable use agreement, I may be subject to disciplinary action. This could include loss of access to the academy network/internet, detentions, suspensions, contact with parents/carers and in the event of illegal activities involvement of the police.

I**f I bring a personal mobile phone or other personal electronic device into the academy:**

- I will not use it during the school day and will either hand it into academy staff (primary academy) or keep it turned off and in a bag (secondary academy).
- If I am a Sixth Form student I will only use my phone for study purposes during the school day and only in designated areas.
- I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online.

Signed (pupil):	**Date:**

Parent/carer's agreement: I agree that my child can use the Trust's ICT systems and internet when appropriately supervised by a member of academy staff. I agree to the conditions set out above for pupils using the Trust's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.

Signed (parent/carer):	**Date:**

Appendix 3: Acceptable Use Agreement (staff, Directors, volunteers and visitors)

ACCEPTABLE USE OF THE TRUST'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, DIRECTORS, VOLUNTEERS AND VISITORS	
Name of staff member/Director/volunteer/visitor:	
The Trust uses Smoothwall filtering and monitoring of all online activities by staff, Directors, volunteers and pupils. More details can be found here. **When using the Trust's ICT systems and accessing the internet in the academy, or outside of it on a work device (if applicable), I will not:** • Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material) • Use them in any way which could harm the Trust's reputation • Access social networking sites or chat rooms unless it is related to a work action which requires this • Use any improper language when communicating online, including in emails or other messaging services • Install any unauthorised software, or connect unauthorised hardware or devices to the Trust's network • Share my password with others or log in to the Trust's network using someone else's details • Take photographs of pupils without checking with the Principal first and never on my own personal device • Share confidential information about the Trust or academy, its pupils or staff, or other members of the community • Access, modify or share data I am not authorised to access, modify or share • Promote private businesses, unless that business is directly related to the Trust or academy	
I will only use the Trust's ICT systems and access the internet in the academy, or outside of it on a work device, for educational purposes or for the purpose of fulfilling the duties of my role. I agree that the Trust will monitor the websites I visit and my use of the Trust's ICT facilities and systems. I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the Trust's data protection policy. I will make use of multi-factor authentication when it is available. I will let the designated safeguarding lead (DSP) and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material. I will always use the Trust's ICT systems and internet responsibly, and ensure that pupils in my care do so too. I have read the Trust's Cyber Security Protocol and understand the role I have to play in keeping the Trust's ICT systems secure.	
Signed (staff/Director/volunteer/visitor):	**Date:**

Appendix 4: Online safety training needs – self audit for staff

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/volunteer:	**Date**:
Question	**Yes/No (add comments)**
Do you know the name of the person who has lead responsibility for online safety in the academy?	
Are you aware of the ways pupils can abuse their peers online?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the Trust's acceptable use agreement for staff, volunteers, Directors and visitors?	
Are you familiar with the Trust's acceptable use agreement for pupils and parents/carers?	
Do you ensure your password for accessing the Trust's ICT systems confirms with the Trust's password policy?	
Are you familiar with the Trust's approach to tackling cyber-bullying?	
Have you read the Trust's Cyber Security Protocol and understand what to do in the event of a cyber-attack?	
Do you understand the filtering and monitoring system the Trust is using when staff and pupils are working online?	
Are there any areas of online safety in which you would like training/further training?	

Appendix 5: Online safety incident report log

Reporting Log Group:						
Date	Time	Incident	Action Taken		Incident Reported By	Signature
			What?	By Whom?		

Training Needs Audit Log Group:				
Relevant training the last 12 months	Identified Training Need	To be met by	Cost	Review Date