# ONLINE SAFETY POLICY

KING EDWARD VI
ASTON SCHOOL

*Educational excellence for our City*

| | |
|---|---|
| **Responsible Board** | **ACADEMY TRUST & FOUNDATION BOARD** |
| **Policy Officer** | **MDO - DSL (EDUCATION & DIGITAL TRANSFORMATION)** |
| **Date Adopted** | **JULY 2022** |
| **Last Reviewed** | **APRIL 2025** |
| **Reviewed by** | **MDO** |
| **Review date** | **APRIL 2026** |

# INTRODUCTION

The Foundation, and King Edward VI Aston School, aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers the Foundation to protect and educate the whole school community in its conduct and use of all technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

# LEGISLATION & GUIDANCE

## Legislation

This policy is based on the Department for Education's statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- teaching online safety in schools
- preventing and tackling bullying
- searching, screening and confiscation

It also refers to the Department's guidance on protecting children from radicalisation: the Prevent Duty. 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.

## Legislation Protecting Personal Data

The Foundation believes that protecting the privacy of our staff and pupils and regulating their safety through data management, control and evaluation is vital to whole-school and individual progress. Schools collect personal data from pupils, parents / carers, and staff and process it in order to support teaching and

learning; monitor and report on pupil and teacher progress; and strengthen pastoral and safeguarding provision.

The Foundation takes responsibility for ensuring that any data that is collected and processed is used correctly and only as is necessary. Parents / carers will be kept fully informed of how data is collected, what is collected, and how it is used. National curriculum results, attendance and registration records, special educational needs data, and any relevant medical information are examples of the type of data that is needed. Through effective data management a range of school provisions, including the wellbeing and academic progression of our pupils, can be monitored and evaluated to ensure that they are being fully supported.

In line with the United Kingdom General Data Protection Regulation ('UK GDPR') and Data Protection Act 2018, and following principles of good practice when processing data, the Foundation will:

- Ensure that data is fairly and lawfully processed;
- Process data only for limited purposes;
- Ensure that all data processed is adequate, relevant and not excessive;
- Ensure that data processed is accurate;
- Not keep data longer than is necessary;
- Process the data in accordance with the data subject's rights;
- Ensure that data is secure;
- Ensure that data is not transferred to other countries without adequate protection.

There may be circumstances where schools are required either by law or in the best interests of pupils or staff to pass information onto external authorities, for example, the local authority, Ofsted, or the Department of Health. These authorities comply with data protection law and have their own policies relating to the protection of any data that they receive or collect.

# ROLES AND RESPONSIBILITIES

## The Trustee Board and Local Governing Body

The Trustee Board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation. The Local Governing

Body will co-ordinate regular meetings with appropriate staff to review online safety incidents and safety logs as provided by the designated safeguarding lead (DSL).
All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's technology and digital systems and the internet (appendix 2)
- 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

## The Headteacher

The Headteacher has a duty of care for ensuring the safety (including digital safety) of members of the school community, and is therefore responsible for:

- ensuring that staff understand this policy, and that it is being implemented consistently throughout the school
- ensuring that the relevant staff receive suitable training to enable them to carry out their digital safety roles
- Being aware of the procedures to be followed in the event of a serious digital safety allegation being made against a member of staff.
- Ensuring appropriate action is taken in all cases of misuse

The Educations and Inspections Act 2006 grants the Headteacher the legal power to take action against incidents affecting the school that occur outside the normal school day and this right will be exercised where it is considered appropriate.

## The Designated Safeguarding Lead (DSL)

The Designated Safeguarding Lead (DSL) - details of the school's designated safeguarding lead (DSL) and any deputies are set out in each school's child protection and safeguarding policy. The DSL should be appropriately trained in digital safety issues.
The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Being aware of the potential for serious child protection / safeguarding issues to arise from sharing of personal data, access to illegal / inappropriate materials, inappropriate digital contact with strangers, incidents of grooming and cyberbullying
- Ensuring that any online safety incidents are logged on CPOMS and dealt with appropriately in line with this policy
- Managing all online safety issues and incidents in line with the school child protection and safeguarding policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety and preventative digital safeguarding measures (appendix 2 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and / or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or Local Governing Body
- Providing regular updates for parents / carers and opportunities for them to engage in training on digital safety
- Ensuring that there are appropriate processes and systems in place for protecting pupils online, e.g., filtering and monitoring This list is not intended to be exhaustive.

## The ICT Manager

The ICT 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 school, including terrorist and extremist material. Details of the current filtering and monitoring in use are available on request

- Ensuring that the school's technology and digital systems are secure and protected against viruses and malware, and that such safety mechanisms are updated and checked regularly
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged on CPOMS and dealt with appropriately in line with this policy
- Ensuring that staff do not have the option to install on school devices any software that is not on the 'allowed' list
- Ensuring that school devices are protected using suitably secure passwords and multi-factor authentication system

This list is not intended to be exhaustive.

## The School community

The School Community - pupils, staff and parents / carers are encouraged not to publish specific and detailed private thoughts, especially those that might be considered hurtful, harmful or defamatory. The Foundation expects all staff, pupils and parents / carers to remember that they are representing the Schools of King Edward VI community at all times and must act appropriately.

All staff, including contractors and agency staff, and volunteers have a duty of care and are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet and ensuring that pupils follow the school's terms on acceptable use (appendix 1)
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and / or harassment, both online and offline and maintaining an attitude of 'it does happen here'
- Ensuring they only use official school-provided email accounts to communicate with pupils, parents / carers and that any communication

should be professionally and carefully written. Staff are representing the school at all times and should take this into account when entering into any email communications.

- Informing their Line Manager or a member of the Leadership Team if they receive any offensive, threatening or unsuitable emails either from within the school or from an external account. They should not attempt to deal with this themselves. Further advice can be sought through The Professionals Online Safety Helpline (POSH) on 0344 381 4772 or via helpline@saferinternet.org.uk

This list is not intended to be exhaustive.

Teachers must also consider their own digital footprint and ensure they adhere to the Teacher Standards.

Outside school, parents / carers bear the same responsibility for guidance as they would normally exercise with information sources such as television, telephones, films, radio and other media. Appropriate home use of the Internet by children can be educationally beneficial, and can make a useful contribution to home and school work. It should, however, be supervised, and parents / carers should be aware that they are responsible for their children's use of Internet resources at home. In addition, if there is a period of school closure which necessitates the wider use of video / audio conferencing to supplement or deliver teaching and learning, the principles of this policy and usual sanctions will apply.

Parents / carers are expected to:

- Notify a member of staff of any concerns or queries regarding this policy or online safety [contact the school directly on 01213271130 or enquiries@ast.kevibham.org].
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendix 1)

Visitors and members of the community who use the school's technology and digital 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.

## Educating Pupils about online safety

It is essential that our pupils are safeguarded from potentially harmful and inappropriate online material. An effective whole school approach to online safety empowers a school to protect and educate pupils and staff in their use of technology and establishes mechanisms to identify, intervene in, and escalate any concerns where appropriate.

The breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk:

- content: being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.
- contact: being subjected to harmful online interaction with other users; for example: child-on-child abuse, 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; for example, making, sending and receiving explicit images (e.g consensual and nonconsensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying;
- commerce - risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your pupils, pupils or staff are at risk, please report it to the Anti-Phishing Working Group

All secondary schools have to teach Relationships and Sex Education and Health Education.

Pupils will be taught about online safety as part of the curriculum. 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
- 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

- Not to provide material to others that they would not want shared further and not to share personal material which is sent to them
- 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)

Pupils in Key Stage 4 will be taught:

- 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 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.

The school will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.
Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

## Educating Parents/Carers about online safety

Parents and carers play a crucial role in ensuring that their children understand the need to use the Internet / mobile devices in an appropriate way. Every opportunity will be taken to help parents/carers understand these issues. The school will raise parents'/carers' awareness of internet safety in letters or other communications home, and in information via the school website. This policy will also be shared with parents/carers.
These letters and communications enable school to keep parents/carers informed and updated regarding the school online filtering and monitoring systems, in addition to outlining our expectations on online tasks, websites and school contacts for pupils. Online safety may also be covered during parents'/carers' evenings.

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 / carer factsheet, Childnet International
- Healthy relationships: Disrespect Nobody
- Report a concern to CEOP that a child is being groomed online or sexually exploited http://www.thinkuknow.co.uk/parents/Get-help/Reporting-an-incident/

## Cyber Bullying

Definition: Cyber-bullying takes place online, such as through social networking sites, messaging apps, chatrooms or gaming sites such as Snapchat, Twitter or TikTok and involves the harassment, threat, embarrassment, intimidation or targeting of someone. 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. Unlike physical bullying, cyber-bullying can often be difficult to track

as the cyber-bully (the person responsible for the acts of cyber-bullying) can remain anonymous when threatening others online, encouraging them to behave more aggressively than they might face-to-face.

## Preventing and addressing cyber-bullying

All our pupils understand our school's approach and are clear about the part they can play to prevent cyber-bullying, including when they should be upstanders not bystanders, and are also made aware of other 'roles' involved in 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. In line with our safeguarding policy, anti-bullying policy, procedures and training, pupils are supported by staff to report cyber-bullying, including where they are a witness rather than the victim, so that they are assured that they will be listened to and incidents acted on.

We do our best to create an inclusive atmosphere in school by encouraging open discussions about the differences between people that could motivate any form of bullying or discrimination, such as religion; ethnicity; disability; gender; sexuality; appearance related difference; different family situations, children being in the care system; or those with caring responsibilities. We also teach our pupils that using any prejudice-based language is unacceptable.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs and the forms it may take. Pupils also know that the school will implement disciplinary sanctions which will reflect the seriousness of the incident so that others see that cyber-bullying is unacceptable and that their behaviour is wrong.

Form tutors will discuss cyber-bullying with their tutor groups, and the issue will be addressed in assemblies.

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.

Staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

The school also sends information / leaflets 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 school will follow the processes set out in the school behaviour policy and Anti-Bullying Policy.
Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavoursto ensure the incident is contained.
The DSL 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.

### Examining electronic devices

School 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. These powers are compatible with Article 8 of the European Convention on Human Rights.
DfE guidance states that parental / carer consent is not required to search through a young person's mobile phone. If a member of staff has reasonable grounds to suspect the device provides evidence that an individual has committed an offence, it should be retained and passed to the police.
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, and/or
- Disrupt teaching, and/or
- Break any of the school rules

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

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or

- 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 and UKCIS guidance on sharing nudes and semi-nudes: advice for education settings
Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

## Acceptable use of internet in school

The Internet is used in school to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions.
All pupils, parents / carers, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1 and 2). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.
Use of school owned and managed hardware, such as computers, to access the 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, governors and visitors (where relevant) to ensure they comply with the above. More information is set out in the acceptable use agreements in appendix 1.

## Pupils using mobile devices in school

The King Edward VI Foundation expects all schools to have a clear policy on the use of mobile and smart technology. Amongst other things this will reflect the fact many children have unlimited and unrestricted access to the internet via mobile phone networks (i.e. 3G, 4G and 5G). This access means whilst at school, child-on-child abuse, bullying or sexual harassment via mobile and smart technology, sharing of indecent images consensually and non-consensually (often via online chat groups) and viewing and sharing pornography and other harmful content may occur. Our schools should carefully consider how this is managed on their premises and reflect this in their mobile and smart technology policy and their child protection and safeguarding policy.

Any pupil who brings a mobile phone or personal device into school is agreeing that they are responsible for its safety. The school will not take responsibility for personal devices that have been lost, stolen or damaged.

King Edward VI Aston School's Electronic Mobile Device policy states that students are allowed to bring devices to school, but they must not be in sight or used between 8.40 and 3.35, or inside the school buildings.

### Staff using school owned and managed devices outside school

Staff members using a work device outside school must not use the device in any way which would violate the school's terms of acceptable use, as set out in [appendix 1] Staff must ensure that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school.
Any USB devices containing data relating to the school must be encrypted. If staff have any concerns over the security of their device, they must seek advice from the ICT manager as soon as possible. If they receive inappropriate contact or content, including threats or defamation, they should report to their Line Manager immediately.

### How the school will respond to issues of misuse

Where a pupil misuses the school's technology and digital systems or internet, we will follow the procedures set out in the behaviour policy. 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 school's technology and digital systems or the internet or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.
The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

### Procedures for staff if they are being cyber bullied

Staff should never respond or retaliate to cyberbullying incidents. They should report incidents appropriately and seek support from a line manager or a senior

member of staff. Evidence of the abuse such as screen shots of messages or web pages should be saved, together with a record of the time and date.
Where the perpetrator is known to be a current pupil or colleague, the majority of cases can be dealt with most effectively through the school's own mediation and disciplinary procedures. Where the perpetrator is known to be an adult, a meeting will be held with the victim to address concerns, and appropriate measures will be taken, including ensuring the offending comments are removed.
Schools or individuals can report the matter to the social networking site if it breaches their terms, or seek guidance from the local authority, legal advisers or support from other agencies for example, The UK Safer Internet Centre or Professional Online Safety Helpline.
If the comments are threatening or abusive, sexist, of a sexual nature or constitute a hate crime, individuals or a representative from the school may consider contacting the local police. Online harassment is a crime.
If staff think they have been affected by a hate crime, they can report it here.

## Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying, sexual violence and harassment, and the risks of online radicalisation.
All staff should be aware of the systems in their school or college which support safeguarding, and these should be explained to them as part of staff induction. As a minimum the KCSIE Part One and the safeguarding and child protection policy will be shared with staff at induction.
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 (for example through emails, ebulletins and staff meetings).
By way of this training, all staff will be made aware that:

- Technology and digital systems is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Child-on-child abuse can occur 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:

- protect themselves
- 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 DSL and any deputies will undertake child protection and safeguarding training, which will include online safety, at least every two years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.
The Headteacher will also undertake child protection and safeguarding training, which will include online safety, at least every two years.
Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.
Volunteers will receive appropriate training and updates, if applicable.
More information about safeguarding training is set out in our child protection and safeguarding policy.

## Monitoring Arrangements

The DSLs log behaviour and safeguarding issues related to online safety.

This policy will be reviewed centrally by the Education Department and locally on an annual basis by the DSL. At every review, the policy will be shared with the Local Governing Body.

## Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy

- Anti-Bullying Policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- Staff Behaviour Guidance

# APPENDIX 1

## Student/Staff/Volunteer Acceptable Use Agreement

In order to safeguard students and staff it is important that all computer system users take all possible measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft. All staff and students have a responsibility to use the school's computer system in a professional, lawful and ethical manner.

By clicking OK and continuing to use this device you are declaring that you have read and will comply with the terms outlined in this acceptable use policy.

- School owned information systems must be used appropriately. I understand that the Computer Misuse Act, 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.
- I understand that any hardware and software provided by the school for staff and student use can only be used by members of the school and only for educational use/practice. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or locking the computer as appropriate.
- I will respect system security and I will not disclose any password or security information. I will not give anyone access to a computer system which I have gained access to. I will use a 'strong' password (including letters and numbers).
- I will not attempt to install any purchased or freely downloaded software, including but not limited to; browser toolbars, extensions, plugins or any other unauthorised applications and hardware without permission from the IT systems manager.
- I understand that the use of VPNs or any systems that circumvent the school's security or internet filtering system is prohibited.
- I am aware of the school's General Data Protection Regulation (EU) 2016/679 (GDPR) Privacy Notice and Data Protection Policy available from the King Edward VI Academy Trust and Aston school website - https://kingedwardvifoundation.co.uk/gdpr
- I have read and understood the school e-safety policy (E-safety policy can be found on school website).
- I will report all incidents of concern to the school's Designated Safeguarding Lead - Mr M Downing.
- If I access school emails on a personal device, I will ensure that the device is 'at least' password protected.

- I will ensure that all sensitive data files sent via email are encrypted/password protected and the password sent via a separate message or over the phone.
- I will not store any sensitive personal documents, files or information on any school owned computer system.
- I will report any suspected data breaches/unauthorised sensitive data access to the school's Data Protection Lead – Mrs K Lally.
- I will respect copyright and intellectual property rights.
- I will report all suspected computer system damage, of virus or other malware to the ICT Department – Mr M Islam and Mr B Wellavize.
- If I am found responsible for any damage to the school's ICT systems that results in financial implications for the school, I may be required to cover the associated costs.
- I am responsible for all email, chat, sms blogs etc. that I post or send and will use language appropriate to the audience who may read them. I will be respectful in how I talk to and work with others online and never write or participate in online bullying. I will report any unpleasant material or messages sent to me. I understand my report will be confidential and may help to protect other students, staff and myself.
- I will not download or bring into school unauthorised programs, including games and videos and run them on school computers/equipment.
- I will not access inappropriate materials such as pornographic, racist or offensive material or use the school system for personal financial gain, gambling, political purposes or advertising.
- I understand that my use of the school information systems is logged.

# APPENDIX 2

## ONLINE SAFETY TRAINING NEEDS – SELF-AUDIT FOR STAFF

| Online safety training needs audit | |
|---|---|
| Name of staff member/volunteer: | Date: |
| Do you know the name of the person who has lead responsibility for online safety in school? | |
| Do you know what you must do if a pupil approaches you with a concern or issue? | |
| Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors? | |

| | |
|---|---|
| How does your school identify and provide relevant online-safety learning to pupils with additional learning needs and vulnerabilities? | |
| Are you familiar with the school's acceptable use agreement for pupils and parents / carers? | |
| Are you familiar with the school's approach to tackling cyber-bullying? | |
| Are there any areas of online safety in which you would like training/further training? Please record them here. | |

# APPENDIX 3

## Terminology:

- AI face transfer technology: AI technology that takes a dataset of photographs of a person, often a celebrity, and generates that person's face on the 3D model. This is sometimes known as 'deepfaking'.
- Augmented Reality (AR): blends the physical world with digital content through smartphones and wearable devices, such as headsets and smart glasses. Common uses include face filters for social media apps, such as Instagram and Snapchat, and location-based games, such as Pokémon Go.
- Avatar: a character that the user inhabits in VR and AR spaces. An avatar can represent a user in real life or be a personal. Users sometimes build a backstory for persona avatars. They are usually highly customisable. Avatar commission: getting a personalised, bespoke avatar designed and produced to use in VR spaces. This commission often involves a payment. Avatar transference, sometimes referred to as mind or consciousness transfer, is a concept in which a person's mind, consciousness, or personality is transferred from their physical body into a digital or artificial one, such as an avatar in a virtual world, a robotic body, or even another biological body. In practical terms, when using a

consumer VR headset, avatar transference is often where a VR avatar temporarily feels as real to a user as their own body.

- Camming: performing on a webcam or other streaming device to a live, online audience.
- Child sexual exploitation (CSE) in augmented reality or virtual reality is the use of immersive technologies to sexually exploit children for commercial gain. This form of CSE involves a child inhabiting an avatar and being exposed to scenarios where they are manipulated into performing sexual content for an individual or audience. This could be through pre-recorded video, interactions in a multi-user VR world, or through live streaming (either on pornography websites or gaming platforms). The anonymising quality of avatars may mean the buyers or viewers of this content do not know the true age of the victim.
- Cryptocurrency: a digital currency in which transactions are verified and records maintained.
- Cyberbullying: harassment, threats or social exclusion through digital means.
- A ‘deep fake’ avatar is one that has been digitally altered to look like a real-life person, such as a celebrity or historic figure. Deep fake avatars can be made to resemble real children, such as a child actor, a family member, or a child in their community, and could potentially be used for malicious purposes (as outlined in the ‘Child sexual abuse simulations in VR’ section of Child Safeguarding & Immersive Technologies: An Outline of the Risks).
- Digital reputation: is the digital footprint created by all the things you say and do online, as well as what others post about you. The people and sites you follow, the content you post, like or share, the comments you make, and what you’re tagged in all contribute to your digital reputation.
- Doomscrolling: compulsively scrolling through content on social media that is depressing or worrying.
- Doxxing: to publicly share a person’s contact details including address without their consent.
- Erotic role play (ERP): refers to the act of users engaging in sexually themed or suggestive interactions while assuming the roles of their chosen avatars within a virtual environment. It can involve various scenarios, characters, and themes and unlike real-world bars and clubs,

entry to ERP in VR spaces is not age restricted. Children under 18 can explore these spaces without supervision.

- Generative artificial intelligence (generative AI, GenAI, or GAI) is artificial intelligence capable of generating text, images, videos, or other data using generative models, often in response to prompts.
- Haptic technology: the use of tactile sensations to stimulate the sense of touch in a user experience, such as vibration in games console controllers.
- Immersive technology, often interchanged with Extended Realities (XR) is the umbrella term for Augmented Reality (AAR), Virtual Reality (VR) and other spatial computing technologies. Many companies position this new wave of tools as the next generation of the internet and suggest that they could be as potentially transformative as social media has been in regard to how we connect with one another.
- Interoperability: the ability of different systems, devices, or software applications to communicate, share, and work with each other effectively. In the context of immersive technologies, it means that assets, contacts, 'friends' or avatars could transfer from one metaverse platform to another. Interoperability inevitably will have implications to child safety on these platforms. It can mean that an offender attempting to groom a child can easily take a multiplatform approach.
- Live action role play: games that take place offline where players adopt fictional characters.
- Machine drift is when we rely on algorithms for our searches. Allowing machine drift poses risks, especially for those who can't tell the difference between reality and fake information or ignore extreme content. Research tells us that children are just 3 clicks away from adult content on platforms like YouTube
- The metaverse refers to the development of an online environment that allows you to take part in day-to day activities that mirror your experience of the 'offline world'. For example, you could go shopping, watch a film at the cinema or have dinner with friends. Some experts have referred to it as a '3D internet'. However, *"[The] metaverse connects users not just to each other but to an array of predators, exposing them to potentially harmful content every seven minutes on average. If the metaverse is safe for predators, it's unsafe for users, especially children."* (Imran Ahmed, Chief Executive of the Centre for Countering Digital Hate)
- Misinformation and fake news: Misinformation is incorrect or misleading information. Fake News are false stories that are deliberately published or

sent around, to make people believe something untrue or to get lots of people to visit a website. These are deliberate lies that are put online, even though the person writing them knows that they are made up. They could also be stories that may have some truth to them, but they're not completely accurate. This is because the people writing them - for example, journalists or bloggers - don't check the facts before publishing the story, or they might exaggerate some of it.

- Offender disinhibition: disinhibition is the state when people feel able to transgress social norms; in the case of VR offenders, it is when they feel safe to commit offences, they may otherwise feel restrained from committing.
- Online grooming or solicitation is defined as the deliberate establishment of an “emotional connection and trust with a child, with the aim of engaging them in sexual behaviour or exploitation using technology.
- Online role play: online games based on storytelling where players take on fictional characters.
- Parasocial relationship is a psychological attachment or connection that an individual forms with a media figure, such as a celebrity, influencer, or fictional character. These relationships develop because of consuming media content.
- Phantom touch: the psychological feeling of touch in VR whereby the brain ‘fills in the gaps’ and believes the person is experiencing physical touch.
- Phishing is a cybercrime in which a target or targets are contacted by email, telephone, or text message by someone posing as a legitimate institution to lure individuals into providing sensitive data such as personally identifiable information, banking and credit card details, and passwords. These deceptive tactics can lead to identity theft, financial loss, and unauthorized access to important accounts.
- Sandbox game refers to a type of video game that provides players with an open-world environment where they can freely explore, create, and interact with the virtual world and its elements without being restricted by a linear narrative or specific objectives. VR sex sandbox games provide a set of tools for creating and animating sexual scenes, designing custom environments, and scripting interactions between characters.
- Sextortion is a form of online blackmail where criminals threaten to share sexual pictures, videos, or information about the victim. They may be trying to take money from the victim or forcing them to do something else

they don't want to. It's essential to recognize the signs, protect yourself, and report any incidents promptly.

- Sexual harassment and assault in VR can be defined as "unwanted, digitally enacted sexual interactions". One form of sexual violence in VR is 'virtual rape', which specifically refers to "a situation in which a user's avatar is forced/coerced into sexual activity against his/her wish". The lack of safeguarding mechanisms in VR spaces, and the failures to implement age limits, means a perpetrator intent on committing sexual assault would not necessarily know the age of the person they are committing the offence against. Without voice cues, it is hard to tell how old someone is by their avatar, as avatar age in VR multiuser worlds does not usually correspond with the actual age of the user.
- Sideloading: the process of transferring files between two local devices, particularly between a personal computer and a mobile device, such as a mobile phone, smartphone, PDA, tablet, or e-reader. Often these sideloaded apps are unapproved or from an unapproved retailer.
- Spoofing is a cyber threat technique involving impersonation of websites, emails, phone numbers, and geolocations to scam, commit financial crimes, or steal identities.
- Virtual assault: also known as 'assault in VR' or 'simulated assault' describes a physical, threatening and unwanted interaction between two or more avatars that does not carry any legal weight.
- Virtual Reality (VR) places users in the centre of a 3D environment where they are surrounded, to experience the sights and sounds of a simulated scenario. VR dissolves the boundary between user and device, giving them a first-person perspective, and a compelling sense of being in the centre of the action. In this context, they are no longer controlling a character, they have become the character. There are a range of activities that children currently take part in through VR without issue, including exercise games and family challenges. It has the potential to be a fantastic educational and social research tool for young people as it can encourage children to develop empathy, help them explore the world around them, and promote fitness. However, research has found that a sizeable minority of children using VR spaces are exposed to the possibility of harm and may, therefore, be at risk.
- Virtual reality child sexual abuse (VR CSA) simulations use immersive technologies to enact child sexual abuse on virtual children. These children are sometimes 3D model depictions of real-life children, such as child actors or children known to the offender. This has obvious

implications for trauma to a child and their family who could learn the child's image is being used in this way. Another form of VR CSA simulation is so-called 'age play', where users 'perform' the role of a child to each other using child avatars to simulate sexual activity. These avatar types are sometimes described as 'loli' (girl) and 'shota' (boy) avatars, and can be bought, sold, and exchanged online. There is evidence that offenders use the fact that VR is virtual to self-justify their actions, often using variations of the phrase "it's just pixels"/ "vegan child porn" to highlight their opinion that it is apparently less harmful.

# APPENDIX 4

## USEFUL LINKS

### Pupils

Children can talk to a ChildLine counsellor 24 hours a day about anything that is worrying them by ringing 0800 1111 or in an online chat at www.childline.org.uk/Talk/Chat/Pages/OnlineChat.aspx

www.childline.org.uk/info-advice/bullying-abuse-safety/digital-mobile-safety/sexting/ Childline support on sexting.

https://www.ditchthelabel.org/living-insta-lie/ An amusing reminder about social media v reality.

Zipit – App allowing young people to send humorous responses to anybody who has asked them to send an explicit image.

### Parents / carers

www.bbc.com/ownit/take-control/own-it-app The Own It app comes with a special keyboard. This can be used like any other keyboard, but it also gives your child helpful tips and friendly advice as they write.

https://www.nspcc.org.uk/keeping-children-safe/online-safety/ Whether you're a digital expert or you're not sure where to start, the NSPCC's tools and advice will help you keep your child safe.

www.saferInternet.org.uk E-safety tips, advice and resources to help children and young people stay safe digital.

http://jcoleman.co.uk/wp-content/uploads/2019/01/SocialMedia.pdf Social media and teenagers. A practical approach. A guide from The Charlie Waller Memorial Trust.

www.commonsensemedia.org To learn more about the games or apps your children are using, Common Sense Media covers thousands, and includes advice and reviews from other parents / carers.

www.thinkuknow.co.uk/parents/articles Advice and information for parents / carers, including links to report concerns.

www.Internetmatters.org Helping parents / carers keep their children safe digitally.

www.net-aware.org.uk Online guide to the social networks, sites and apps children use.

www.childnet.com Non-profit organisation working with others to help make the Internet a great and safe place for children.

www.iwf.org.uk Internet Watch Foundation receive, assess and trace public complaints about child sexual abuse content on the internet and support the development of website rating systems. It is also the UK hotline for reporting criminal online content with particular reference to images of child sexual abuse.

http://parentinfo.org/article/where-do-i-report-if-im-worried-about-my-childs-safety-digital A parent's / carer's guide to help report digital activity.

www.parentsprotect.co.uk Provides information and resources for parents / carers about child sexual abuse, including a section on online safety.

www.gov.uk/government/uploads/system/uploads/attachment_data/file/490001/Social_Media_Gu idance_UKCCIS_Final_18122015.pdf.pdf Child Safety Digital: A practical guide for parents and carers whose children are using social media.

www.snapchat.com/l/en-gb/safety/ and www.parentinfo.org/article/snapchat-what-to-do-if-you-reworried Snapchat digital safety.

www.lifewire.com/what-is-instagram-3486316 What is Instagram and how is it used?

www.lifewire.com/what-is-snapchat-3485908 What is Snapchat and how is it used?

www.connectsafely.org/a-parents-guide-to-mobile-phones A parent's/carer's guide including tips for Smartphone use; helping children protect their safety, privacy and security; and parental controls.

www.connectsafely.org/wp-content/uploads/A-Parent's-Guide-to-Snapchat.pdf A parent's / carer's guide to Snapchat (US version). Note UK support address on page 5 is: https://support.snapchat.com/en-GB/i-need-help

http://www.connectsafely.org/familylink/ This guide provides parents / carers with an overview of the Family Link parental tools with tips on how to set up and manage their child's device, including setting "screen time" to determine how long and at what times they can use their device.

www.connectsafely.org/fakenews A parent / carer and educator guide to media literacy and fake news.

www.childrenscommissioner.gov.uk/publication/life-in-likes/ This Children's Commissioner's report on the effects of social media on 8-to-12-year-olds examines the way children use social media and its effects on their wellbeing. 'Life in Likes' fills a gap in research showing how younger children use platforms which social media companies say are not designed for them.

www.esafety-adviser.com/latest-newsletter/ Teachers or parents / carers can sign up to the newsletter which comes out every 6 weeks.

www.bps.org.uk/news-and-policy/changing-behaviour-children-adolescents-and-screen-use Paper from the British Psychological Society (2018). The recommendations set out in the paper recognise that the issue of children's digital media use is more complex than amount of screen time and acknowledges both benefits and risks to media use.

## Staff

https://digital-literacy.org.uk/ South West Grid for Learning provide free materials designed to empower pupils to think critically, behave safely, and participate responsibly in our digital world. Browse by Key Stage or Year Group, for cross-curricular lessons which address digital literacy and citizenship topics in an age-appropriate way.

www.gov.uk/government/publications/education-for-a-connected-world The Education for a Connected World framework describes the Digital knowledge and skills that children and young people should have the opportunity to develop at different ages and stages of their lives. It highlights what a child should know in terms of current online technology, its influence on behaviour and development, and what skills they need to be able to navigate it.

www.gov.uk/government/groups/uk-council-for-child-internet-safety-ukccis The UK Council for Child Internet Safety is now the UK Council for Internet Safety (UKCIS)

www.gov.uk/government/publications/teaching-online-safety-in-schools 2019 guidance supporting schools to teach pupils how to stay safe online when studying new and existing subjects.

www.ofcom.org.uk/__data/assets/pdf_file/0024/149253/online-nation-summary.pdf - Online Nation is a new annual report that looks at what people are doing online, how they are served by online content providers and platforms, and their attitudes to and experiences of using the internet. It brings the relevant research into a single place and aims to act as a data- and insight driven resource for stakeholders at a time of significant evolution in the online landscape.

www.e-safetysupport.com/resources/details/?resource_type=support_advice What every teacher needs to know about e-safety.

https://pwxp5srs168nsac2n3fnjyaa-wpengine.netdna-ssl.com/wp-content/uploads/2019/02/Vulnerable-Children-in-a-Digital-World-FINAL.pdf This study looks at a number of vulnerable groups in order to ascertain differences of experiences and vulnerabilities.

www.rsph.org.uk/our-work/policy/wellbeing/new-filters.html Report by the All Party Parliamentary Group (APPG) on Social Media on the Group's Inquiry, "#NewFilters to manage the impact of social media on young people's mental health and wellbeing". This is the first national Inquiry specifically examining the impact of social media on the mental health and wellbeing of young people, which ran from April 2018 to January 2019.

www.thinkuknow.co.uk/professionals/ Supporting you to deliver education and raise awareness of digital child exploitation and abuse.

www.thinkuknow.co.uk/professionals/guidance/digital-romance/ This research project looks at how young people use technology in developing romantic relationships and surviving break ups. The project was led by Brook, the UK's leading sexual health and wellbeing charity for under 25s, and the CEOP Command of the NCA.

www.tes.com/teaching-resource/digital-citizenship-young-peoples-rights-on-social-media-teaching-pack-for-11-14-year-olds-11734349 Digital citizenship: Young peoples' rights on social media – a teaching pack designed to help pupils aged 11 to 14 develop the resilience, power and information they need to thrive online. This teaching pack comprises a short, six-lesson unit of work written by teacher and citizenship specialist Emily Cotterill.

www.nen.gov.uk/digital-safety Leading educational support for helping you stay safe digitally. https://educateagainsthate.com/ This website gives teachers, parents and school leaders practical advice and information on protecting children from extremism and radicalisation.

www.gov.uk/government/uploads/system/uploads/attachment_data/file/440450/How_social_media_is_used_to_encourage_travel_to_Syria_and_Iraq.pdf This briefing note is aimed at head teachers, teachers and safeguarding leads and provides advice about digital terrorist and extremist material.

www.mercurynews.com/2017/09/21/how-to-combat-lgbtq-cyberbullying Article on combating LGBTQ+ bullying.

https://www.barnardos.org.uk/campaign-with-us/childrens-social-media-and-mental-health Report on children's social media and mental health.

https://www.gov.uk/government/publications/sexting-in-schools-and-colleges 'Sexting' in schools: advice and support around self-generated images. This advice is for designated safeguarding leads (DSLs), their deputies, head teachers and senior leadership teams in schools and educational establishments.

www.gov.uk/government/uploads/system/uploads/attachment_data/file/650933/Literature_Review_Final_October_2017.pdf Children's digital activities, risks and safety. A literature review by the UKCCIS (UK Council for Child Internet Safety) Evidence Group. October 2017.

https://www.gov.uk/government/publications/digital-resilience-framework A framework and tool for organisations, policymakers, schools and companies to use to embed digital resilience thinking into products, education and services.

The NSPCC Knowledge and Information Services provide newsletters and updates on safeguarding research, including digital safety. Information can be found at www.nspcc.org.uk/library CASPAR (Current Awareness Service for Policy, Practice and Research) is the NSPCC's weekly email update delivering the latest news in child protection policy, practice and research, every Monday. Sign up to CASPAR at www.nspcc.org.uk/caspar or you can follow them on Twitter @NSPCCpro. The NSPCC also provide specialist child protection courses (introductory, advanced and specialist) either online or face-to-face www.nspcc.org.uk/training